INTERNET SECURITY 2012

Handleiding

Bitdefender Internet Security 2012
Handleiding

Publication date 2011.07.27

Wettelijke bepaling


Bitdefender

Inhoudsopgave

1. Installatie

1.1. Voorbereiden voor installatie

Voordat u Bitdefender Internet Security 2012 installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de computer waarop u Bitdefender wilt installeren, voldoet aan de minimale systeemvereisten.Als de computer niet voldoet aan alle minimale systeemvereisten, wordt Bitdefender niet geïnstalleerd. Als het programma als is geïnstalleerd, zal het niet goed werken en zal het systeem vertragen en instabiel worden.Raadpleeg *"Systeemvereisten" (p. 1)* voor een complete lijst van systeemvereisten.
- Meld u aan bij de computer met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de computer.Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken.Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- Schakel alle firewall-programma's die mogelijk op uw computer worden uitgevoerd uit of verwijder ze.Als u twee firewallprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken.Windows Firewall zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw computer verbonden te laten met internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert.Indien er nieuwere versies van de toepassingsbestanden dan die in het installatiepakket beschikbaar zijn, zal Bitdefender deze downloaden en installeren.

1.2. Systeemvereisten

U kan Bitdefender Internet Security 2012 uitsluitend installeren op computers met de volgende besturingssystemen:

- Windows XP met Service Pack 3 (32-bit)
- Windows Vista met Service Pack 2
- Windows 7 met Service Pack 1

Controleer vóór de installatie of uw computer voldoet aan de minimum systeemvereisten.

Opmerking

Om het Windows besturingsssysteem en de hardware-informatie van uw computer te zien, rechtsklikt u op **Deze Computer** op het bureaublad en selecteert u **Eigenschappen** in het menu.

1.2.1. Minimale systeemvereisten

- 1,8 Gb beschikbare vrije ruimte op de harddisk (ten minste 800 Mb op de systeemschijf)
- Processor 800 MHz
- 1 Gb geheugen (RAM)

1.2.2. Aanbevolen systeemvereisten

- 2,8 Gb beschikbare vrije ruimte op de harddisk (ten minste 800 Mb op de systeemschijf)
- Intel CORE Duo (1,66 GHz) of equivalente processor
- Geheugen (RAM):
  - 1 Gb voor Windows XP
  - 1.5 Gb voor Windows Vista en Windows 7

1.2.3. Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw computer voldoen aan de volgende softwarevereisten:

- Internet Explorer 7 of hoger
- Mozilla Firefox 3.6 of hoger
- Yahoo! Messenger 8.1 of hoger
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express en Windows Mail (op 32-bits systemen)
- Mozilla Thunderbird 3.0.4
- .NET Framework 3

1.3. Uw Bitdefender-product installeren

U kunt Bitdefender installeren vanaf de installatie-cd van Bitdefender, met het webinstallatiebestand dat u van de Bitdefender-website hebt gedownload naar uw computer of vanaf andere gemachtigde websites (bijvoorbeeld de website van een Bitdefender-partner of een online winkel).U kunt het installatiebestand downloaden van de Bitdefender-website op het volgende adres: http://www.bitdefender.com/site/Downloads/.

- Om Bitdefender te installeren vanaf de installatieschijf, plaatst u de schijf in het optische station.Na enkele ogenblikken zou een welkomstscherm moeten worden weergegeven. Volg de instructies om de installatie te starten.

Opmerking

Het welkomstscherm biedt een optie voor het kopiëren van het installatiepakket vanaf de installatieschijf naar een USB-opslagapparaat.Dit is nuttig als u Bitdefender moet installeren op een computer die geen schijfstation heeft (bijv. op een netbook).Voeg het opslagapparaat in de USB rit in en klik dan **Kopie naar USB**.Ga daarna naar de computer zonder schijfstation, plaats het opslagapparaat in het USB-station en dubbelklik op `runsetup.exe` in de map waarin u het installatiepakket hebt opgeslagen.

Als het welkomstscherm niet verschijnt, gaat u naar de hoofdmap van de schijf en dubbelklikt u op het bestand `autorun.exe`.

- Om Bitdefender te installeren met het webinstallatiebestand dat op uw computer is gedownload, zoekt u het bestand en dubbelklikt u erop.Hierdoor zal het downloaden van de installatiebestanden starten. Dit kan even duren, afhankelijk van uw internetverbinding.

Bitdefender zal uw systeem eerst controleren om de installatie te valideren.

Als uw systeem niet voldoet aan de minimumvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibel antivirusprogramma of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen.Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden.

Opmerking

U zult mogelijk uw computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde antivirusprogramma's te voltooien.

Volg de installatiewizard voor het installeren van Bitdefender Internet Security 2012.

Stap 1 - Welkom

Lees de licentieovereenkomst en selecteer **Akkoord & Doorgaan**.De licentieovereenkomst bevat de voorwaarden en bepalingen voor uw gebruik van Bitdefender Internet Security 2012.

Opmerking

Sluit het venster als u niet akkoord gaat met deze voorwaarden.Het installatieproces wordt afgebroken en u verlaat de installatie.

Stap 2 - Uw product registreren

Om de registratie van uw product te voltooien, dient u een licentiesleutel in te voeren en een MyBitdefender-account aan te maken.Er is een actieve internetverbinding vereist.

Ga verder volgens uw situatie:

- **Ik heb het product gekocht**

  Registreer het product in dit geval door de volgende stappen te volgen:

  1. Selecteer **Ik heb het product gekocht en ik wil het nu registreren**.
  2. Typ de licentiesleutel in het overeenkomstige veld in.

     Opmerking

     U kan uw licentiesleutel vinden:
     - op het cd/dvd-label.
     - op de productregistratiekaart.
     - in de online aankoop e-mail.

  3. Typ uw e-mailadres in het overeenkomende veld in.

     Belangrijk

     Er is een geldig e-mailadres vereist.Er zal een bevestigingsbericht naar het adres dat u hebt opgegeven worden verzonden.

  4. Klik op **Nu registreren**.

- **Ik wil graag Bitdefender evalueren**

  In dit geval kunt u het product gedurende 30 dagen gebruiken.Om de evaluatieperiode te starten, selecteert u **Ik wil dit product evalueren**.

  Om de online functies van het product te kunnen gebruiken, dient u een MyBitdefender account aan te maken.Om een account aan te maken, typt u uw e-mailadres in het overeenkomstige veld in.Er zal een bevestigingsbericht naar het adres dat u hebt opgegeven worden verzonden.Indien u al een account hebt, voert u het e-mailadres dat daarbij hoort in om het product bij die account te registreren.

Instellingen aanpassen

Optioneel kunt u tijdens deze stap de instellingen voor de installatie ook aanpassen door op **Aangepaste instellingen** te klikken.

Installatiepad

Standaard wordt Bitdefender Internet Security 2012 geïnstalleerd in `C:\Program Files\Bitdefender\Bitdefender 2012`.Als u het

installatiepad wilt wijzigen, klikt u op **Wijzigen** en selecteert u de map waarin u Bitdefender wilt installeren.

Proxy-instellingen configureren

Bitdefender Internet Security 2012 vereist internettoegang voor productregistratie, het downloaden van beveiligings- en productupdates, “in-the-cloud”-detectie van componenten, enz.Als u een Proxyverbinding gebruikt in plaats van een directe internetverbinding, moet u deze optie selecteren en de proxy-instellingen configureren.

De instellingen kunnen worden geïmporteerd vanaf de standaardbrowser of u kunt ze handmatig invoeren.

P2P update inschakelen

U kunt de productbestanden en handtekeningen met andere Bitdefender-gebruikers delen.Op deze manier kunnen Bitdefender-updates sneller worden uitgevoerd.Als u deze functie niet wilt inschakelen, schakelt u het overeenkomende selectievakje in.

Opmerking

Als deze functie is ingeschakeld, wordt er geen persoonlijke identificeerbare informatie gedeeld.

Als u de invloed van het netwerkverkeer op uw systeemprestaties tijdens updates wilt minimaliseren, kunt u de optie voor het delen van updates gebruiken.Bitdefender gebruikt poorten 8880 - 8889 voor peer-to-peer update.

Anonieme gebruiksverslagen verzenden

De optie Anonieme gebruiksverslagen is standaard ingeschakeld.Door deze optie in te schakelen, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden.Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden.Merk op dat deze rapporten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

Klik op **OK** om uw voorkeuren te bevestigen.

Klik op **Installeren** om de installatie te starten.

Stap 3 - Installatievoortgang

Wacht tot de installatie is voltooid.Er wordt gedetailleerde informatie over de voortgang weergegeven.

Kritieke zones op uw systeem worden gescand op virussen, de nieuwste versies van de toepassingsbestanden worden gedownload en geïnstalleerd en de services van Bitdefender worden gestart. Deze stap kan enkele minuten duren.

Stap 4 - Voltooien

Er wordt een overzicht van de installatie weergegeven.Als tijdens de installatie een actieve malware wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

Klik op **Voltooien**.

Als uw computer werkt met Windows XP, detecteert de installatiewizard alle netwerken waarmee u verbonden bent en wordt u gevraagd ze te classificeren als Thuis/Kantoor of Openbaar.

1.3.1. Bezig met upgraden van een oudere versie

Indien u al een oudere versie van Bitdefender gebruikt, zijn er twee manieren om te upgraden naar Bitdefender Internet Security 2012:

- Bitdefender Internet Security 2012 rechtstreeks over de oudere versie installeren.Bitdefender zal de oudere versie detecteren en zal u helpen om deze te verwijderen voordat de nieuwe versie wordt geïnstalleerd.U zult de computer opnieuw op moeten starten tijdens de upgrade.
- Verwijder de oudere versie. Start de computer dan opnieuw op en installeer de nieuwe versie, zoals beschreven op de vorige pagina's.Gebruik deze upgrademethode als de andere mislukt.

Opmerking

De productinstellingen en quarantaine-inhoud zal niet worden geïmporteerd van de oudere versie.

2. Aan de slag

Nadat u Bitdefender Internet Security 2012 hebt geïnstalleerd, wordt uw computer beschermd tegen alle types malware (zoals virussen, spyware en Trojaanse paarden) en internetbedreigingen (zoals hackers, phishing en spam).

Auto pilot is standaard ingeschakeld en u hoeft geen instellingen te configureren.U kunt echter voordeel halen uit de Bitdefender-instellingen om uw beveiliging fijn af te stemmen en te verbeteren.

Bitdefender zal de meeste beslissingen met betrekking tot de beveiliging voor u nemen en zal zelden pop-upwaarschuwingen weergeven.Details over acties die worden ondernomen en informatie over de programmabediening zijn beschikbaar in het venster Gebeurtenissen.Meer informatie vindt u onder “*Gebeurtenissen*” (p. 13).

Het is aanbevolen Bitdefender af en toe te openen en de bestaande problemen te herstellen.U zult mogelijk specifieke Bitdefender-componenten moeten configureren of preventieve acties ondernemen om uw computer en gegevens te beschermen.

Als u het product niet hebt geregistreerd (en geen MyBitdefender-account hebt gemaakt), moet u dit doen voordat de evaluatieperiode verloopt.U moet een account maken om de online functies van het product te gebruiken.Raadpleeg “*Productregistratie*” (p. 8) voor meer informatie over het registratieproces.

2.1. Bitdefender openen

De hoofdinterface van Bitdefender Internet Security 2012 is toegankelijk via het volgende pad vanaf het menu Start van Windows: **Start → Alle programma's → Bitdefender 2012 → Bitdefender Internet Security 2012**. Dit kan sneller door in het systeemvak te dubbelklikken op het Bitdefender-pictogram  .

Meer informatie over het Bitdefender-venster en -pictogram in het systeemvak, vindt u op “*Bitdefender-interface*” (p. 20).

2.2. Dit moet u doen na de installatie

Als u wilt dat Bitdefender alle beveiligingsverwante beslissingen voor u neemt, moet u Auto Pilot ingeschakeld houden.Meer informatie vindt u onder “*Auto Pilot*” (p. 14).

Hier vindt u een lijst van de taken die u mogelijk wilt uitvoeren na de installatie:

- Als uw computer een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in “*Bitdefender configureren voor het gebruik van een proxy-internetverbinding*” (p. 37).

- Als u Bitdefender op meerdere computers in uw thuisnetwerk hebt geïnstalleerd, kunt u alle Bitdefender-producten op afstand beheren vanaf één computer.Meer informatie vindt u onder "*Netwerk map*" (p. 107).
- Als u kinderen hebt, kunt u Ouderlijk toezicht gebruiken om te bewaken en te beheren wat ze doen op de computer en op internet.Ouderlijk toezicht is standaard ingeschakeld voor beperkte Windows-gebruikersaccounts en de regels voor de webfilter, geschikt voor tieners, worden toegepast.Meer informatie vindt u onder "*Ouderlijk Toezicht*" (p. 82).
- Maak regels voor de Gegevensbeveiliging om te voorkomen dat belangrijke persoonlijke gegevens worden bekendgemaakt zonder uw toestemming.Meer informatie vindt u onder "*Data bescherming*" (p. 78).

2.3. Productregistratie

Als u wilt dat u door Bitdefender wordt beschermd, moet u uw product registreren door een licentiesleutel in te voeren en een MyBitdefender-account te maken.

De licentiesleutel bepaalt hoelang u het product mag gebruiken.Zodra de licentiesleutel vervalt, stopt Bitdefender met het uitvoeren van zijn functies en het beschermen van uw computer.

Enkele dagen voordat de huidige licentiesleutel aanschaft of vernieuwt, moet u een licentiesleutel aanschaffen of uw licentie vernieuwen.Meer informatie vindt u onder "*Licentiesleutels kopen of vernieuwen*" (p. 11).Als u een evaluatieversie van Bitdefender gebruikt, moet u deze registreren met een licentiesleutel als u product wilt blijven gebruiken nadat de evaluatieperiode is verlopen.

Een MyBitdefender-account biedt u toegang tot productupdates en biedt u de mogelijkheid de online-services die door Bitdefender Internet Security 2012 worden geboden, te gebruiken.Als u al een account hebt, moet u uw Bitdefender-product registreren voor die account.

Met een MyBitdefender-account kunt u het volgende doen:

- Houd uw product up-to-date.
- U kunt uw licentiesleutel ophalen als u deze ooit zou vergeten.
- Neem contact op met de klantendienst van Bitdefender.
- Bewaak de activiteiten van uw kinderen en configureer de instellingen voor Ouderlijk toezicht waar u ook bent.
- Geniet van bescherming van uw Facebook-account met Safego.

2.3.1. Uw licentiesleutel invoeren

Als u tijdens de installatie hebt gekozen om het product te evalueren, kunt u dit gedurende een evaluatieperiode van 30 dagen gebruiken.Om Bitdefender verder

te blijven gebruiken na het verlopen van de evaluatieperiode, moet u het registreren met een licentiesleutel.

Om het product te registreren met een licentiesleutel of als u de huidige licentiesleutel wilt wijzigen, klikt u op de koppeling **Informatie licentie** onderaan in het Bitdefender-venster.Het registratievenster wordt weergegeven.

U kan de Bitdefender registratiestatus zien, evenals de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

Bitdefender Internet Security 2012 registreren:

1. Typ de licentiesleutel in het bewerkingsveld.

Opmerking

U kan uw licentiesleutel vinden:

- op het cd label.
- op de productregistratiekaart.
- in de online aankoop e-mail.

Als u geen Bitdefender-licentiesleutel hebt, klikt u op de koppeling die in het venster is voorzien om een webpagina te openen waar u een sleutel kunt aanschaffen.

2. Klik op **Nu registreren**.

2.3.2. Aanmelden bij MyBitdefender

Als u tijdens de installatie een e-mailadres hebt opgegeven, hebt u een bevestigings-e-mail ontvangen op het opgegeven adres.Klik op de koppeling in de e-mail om de registratie te voltooien.

Als u de registratie niet hebt voltooid, zal Bitdefender een bericht weergeven met de vraag dit alsnog te doen.

Belangrijk

U moet zich binnen 30 dagen na het installeren van Bitdefender aanmelden bij een account.Anders zullen er geen updates van Bitdefender meer worden uitgevoerd.

Voor het aanmaken of aanmelden bij een MyBitdefender-account, klikt u op de koppeling **Registratie voltooien** / **MyBitdefender** onderaan in het Bitdefender-venster.

Het MyBitdefender-venster wordt geopend.Ga verder volgens uw situatie.

Ik wil een MyBitdefender-account maken.

Volg deze stappen om een MyBitdefender-account te maken:

1. Selecteer **Nieuwe account aanmaken**.

Een nieuw venster wordt weergegeven.

2. Typ de vereiste informatie in de overeenkomende velden.De gegevens die u hier opgeeft blijven vertrouwelijk.
   - **Naam** - voer een gebruikersnaam in voor uw account. Dit veld is optioneel.
   - **E-mail** - voer uw e-mailadres in.
   - **Wachtwoord** - voer een wachtwoord in voor uw account.Het wachtwoord moet minstens 6 tekens lang zijn.
   - **Wachtwoord bevestigen** - typ het wachtwoord opnieuw.
   - Optioneel kan Bitdefender u informeren over speciale aanbiedingen via het e-mailadres van uw account.Om deze optie in te schakelen, selecteert u **Ik geen Bitdefender de toestemming om mij e-mails te sturen**.

   Opmerking
   Zodra de account is gemaakt, kunt u het bijgeleverde e-mailadres en het wachtwoord gebruiken om u aan te melden bij uw account op http://my.bitdefender.com.

3. Klik op **Verzenden**.
4. Voordat u uw account kunt gebruiken, moet u de registratie voltooien.Controleer uw e-mail en volg de instructies in de bevestigings-e-mail die u ontvangen hebt van Bitdefender.

Opmerking
U kunt zich ook aanmelden met uw Facebook- of Google-account.Meer informatie vindt u onder"Ik wil mij aanmelden met mijn Facebook- of Google-account" (p. 10)

Ik wil mij aanmelden met mijn Facebook- of Google-account

Volg deze stappen om u aan te melden bij uw Facebook- of Google-account.

1. Klik op het pictogram van de service die u wilt gebruiken om aan te melden.U wordt omgeleid naar de aanmeldingspagina van die service.
2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.

Opmerking
Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

Ik heb al een MyBitdefender-account

Als u zich eerder bij een account hebt aangemeld vanaf uw product, zal Bitdefender dit detecteren en u aanmelden bij die account.U kunt uw account op http://my.bitdefender.com bezoeken door op **Ga naar MyBitdefender** te klikken.

Als u wilt aanmelden bij een andere account, klikt u op de overeenkomende koppeling en volgt u de instructies in de vorige onderdelen.

Als u al een actieve account hebt, maar Bitdefender deze niet detecteert, moet u deze stappen volgen om u aan te malden bij die account:

1. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.

   Opmerking
   Als u uw wachtwoord bent vergeten, klikt u op **Wachtwoord vergeten** en volgt u de instructies om het op te halen.

2. Klik op **Aanmelden**.

2.3.3. Licentiesleutels kopen of vernieuwen

Als de evaluatieperiode binnenkort zal eindigen, moet u een licentiesleutel aanschaffen en uw product registreren.Zo moet u ook uw licentie vernieuwen als uw huidige licentiesleutel binnenkort vervalt.

Bitdefender zal u waarschuwen wanneer de vervaldatum van uw huidige licentie nadert. Volg de instructies in de waarschuwing om een nieuwe licentie aan te schaffen.

U kunt een webpagina bezoeken waar u op elk ogenblik een licentiesleutel kunt aanschaffen door deze stappen te volgen:

1. Open het Bitdefender-venster.
2. Klik op de koppeling **Informatie licentie** onderaan in het Bitdefender-venster om het productregistratievenster te openen.
3. Klik op de hiervoor voorziene koppeling in het onderste gedeelte van het venster.

2.4. Problemen aan het oplossen

Bitdefender gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de problemen die de veiligheid van uw computer en gegevens kunnen beïnvloeden. Standaard zal het programma alleen een reeks problemen bewaken die als zeer belangrijk worden beschouwd. U kunt dit echter configureren volgens uw behoeften, waarbij u specifieke problemen kunt kiezen waarvan u op de hoogte wilt worden gebracht.

De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen. Ze zijn gegroepeerd in twee categorieën:

- **Kritieke problemen** - verhinderen dat Bitdefender u beveiligt tegen malware of vormen een belangrijk beveiligingsrisico.
- **Minder belangrijke (niet-kritieke) problemen** - kan uw beveiliging in de nabije toekomst beïnvloeden.

Het Bitdefender-pictogram in het systeemvak geeft problemen in behandeling aan door de kleur als volgt te wijzigen:

Rood: Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

Geel: Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.

Als u de muiscursor over het pictogram beweegt, verschijnt bovendien een pop-up dat het bestaan van problemen in behandeling bevestigt.

Wanneer u het Bitdefender-venster opent, geeft het gebied Beveiligingsstatus in de werkbalk bovenaan het aantal en de aard van de problemen die uw systeem beïnvloeden aan.

2.4.1. Wizard alle problemen herstellen

Volg de wizard **Alle problemen herstellen** om de gedetecteerde problemen op te lossen.

1. Voer een van de volgende bewerkingen uit om de wizard te openen:
   - Klik met de rechtermuisknop op het Bitdefender-pictogram in het systeemvak en selecteer **Alle problemen herstellen**.Afhankelijk van de gedetecteerde problemen is het pictogram rood (wat wijst op kritieke problemen) of geel (wat wijst op niet-kritieke problemen).
   - Open het Bitdefender-venster en klik op een willekeurige plaats binnen het gebied Beveiligingsstatus in de werkbalk bovenaan (u kunt bijvoorbeeld op de knop **Alle problemen herstellen** klikken).
2. U kunt de problemen zien die de veiligheid van uw computer en gegevens beïnvloeden.Alle huidige problemen zijn geselecteerd om te worden opgelost.

   Als u een specifiek probleem niet meteen wilt oplossen, schakelt u het overeenkomende selectievakje uit.U wordt gevraagd op te geven hoelang het oplossen van het probleem kan worden uitgesteld.Kies de gewenste optie in het menu en klik op **OK**.Kies **Permanent** om de bewaking van de respectieve problemencategorie te stoppen.

De status van het probleem verandert naar **Uitstellen** en er wordt geen actie ondernomen om het probleem op te lossen.

3. Om de geselecteerde problemen op te lossen, klikt u op **Start**. Sommige problemen worden onmiddellijk opgelost. Bij andere problemen wordt u geholpen door een wizard om ze op te lossen.

De problemen die deze wizard u helpt oplossen kunnen in deze hoofdcategorieën worden gegroepeerd.

- **Uitgeschakelde beveiligingsinstellingen.** Dergelijke problemen worden onmiddellijk opgelost door hun respectievelijke beveiligingsinstellingen in te schakelen.
- **Preventieve beveiligingstaken die u moet uitvoeren.** Wanneer u dergelijke problemen oplost, helpt een wizard u bij het voltooien van de taak.

2.4.2. Statuswaarschuwingen configureren

Het statuswaarschuwingssysteem is vooraf geconfigureerd voor de bewaking en om u te waarschuwen voor de belangrijkste problemen die de veiligheid van uw computer en gegevens kunnen beïnvloeden.Naast de problemen die standaard worden bewaakt, zijn er verschillende andere problemen waarover u op de hoogte kunt worden gebracht.

U kunt het waarschuwingssysteem configureren om optimaal te voldoen aan uw beveiligingsbehoeften door te kiezen over welke problemen u op de hoogte wilt worden gebracht.Volg deze stappen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Geavanceerd**.
4. Zoek en klik op de koppeling **Statuswaarschuwingen configureren**.
5. Klik op de schakelaars om de statuswaarschuwingen volgens uw voorkeuren in of uit te schakelen.

2.5. Gebeurtenissen

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer (ook inclusief computeractiviteiten die worden bewaakt door Ouderlijk toezicht).Gebeurtenissen zijn een zeer belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging.U kan bijvoorbeeld gemakkelijk controleren of de update is gelukt, of er malware op uw computer is gevonden, enz.Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.

Om het venster Gebeurtenissen te openen, opent u het Bitdefender-venster en klikt u in de werkbalk bovenaan op de knop **Gebeurtenissen**.

Om u te helpen de gebeurtenissen van Bitdefender te filteren, zijn de volgende categorieën beschikbaar in het menu aan de linkerzijde:

- **Antivirus**
- **Antispam**
- **Ouderlijk Toezicht**
- **Privacybeheer**
- **Firewall**
- **Netwerk map**
- **Update**
- **SafeGo**
- **Registratie**

Voor elke categorie is een lijst gebeurtenissen beschikbaar.U kunt meer informatie over een specifieke gebeurtenis in de lijst weergeven door erop te klikken. Details over de gebeurtenis worden weergegeven in het onderste deel van het venster.Elke gebeurtenis biedt de volgende informatie: een korte beschrijving, de actie die Bitdefender heeft genomen wanneer de gebeurtenis is opgetreden en de datum en het tijdstip van de gebeurtenis.Er kunnen opties worden geboden voor het ondernemen van verdere actie.

U kunt gebeurtenissen filteren volgens hun belang.Er zijn drie types gebeurtenissen. Elk type wordt aangeduid door een specifiek pictogram:

Gebeurtenissen van het type **Informatie** duiden op een geslaagde bewerking.
Gebeurtenissen van het type **Waarschuwing** wijzen op niet-kritieke problemen. U moet ze controleren en herstellen wanneer u tijd hebt.
Kritieke gebeurtenissen wijzen op kritieke problemen. U moet ze onmiddellijk controleren.

Om u te helpen geregistreerde gebeurtenissen gemakkelijker te beheren, biedt elk deel van het venster Gebeurtenissen opties waarmee alle gebeurtenissen in dat deel kunnen worden verwijderd of gemarkeerd als gelezen.

2.6. Auto Pilot

Voor alle gebruikers die van hun beveiligingsoplossing alleen vragen dat ze worden beschermd zonder te worden gehinderd, werd Bitdefender Internet Security 2012 ontworpen met een ingebouwde Auto pilot-modus.

Wanneer u in de modus Auto pilot bent, past Bitdefender een optimale beveiligingsconfiguratie toe en neemt de toepassing alle beslissingen met betrekking tot de beveiliging voor u.Dit betekent dat u geen pop-upberichten of waarschuwingen zult zien en dat u geen enkele instelling zult moeten configureren.

In de modus Auto Pilot, lost Bitdefender automatisch kritieke problemen op en beheert het op de achtergrond:

- Antivirusbeveiliging, geleverd door Scannen bij toegang en Doorlopend scannen.
- Firewallbeveiliging.
- Privacybescherming, geleverd door antiphishing- en antimalware-filters voor het surfen op het web.
- Automatische updates.

Auto pilot wordt standaard ingeschakeld zodra de installatie van Bitdefender is voltooid.Zolang Auto pilot is ingeschakeld, verandert het Bitdefender-pictogram in het systeemvak naar .

Om Auto Pilot in of uit te schakelen, opent u het Bitdefender-venster en klikt u op de schakelaar **Auto Pilot** in de werkbalk bovenaan.

Belangrijk
Wanneer Auto Pilot is ingeschakeld en u instellingen die door deze toepassing worden beheerd wijzigt, zal Auto Pilot worden uitgeschakeld.

Open het venster Gebeurtenissen om de geschiedenis te zien van acties die door Bitdefender zijn ondernomen terwijl Auto Pilot is ingeschakeld.

2.7. Spelmodus en Laptop-modus

Sommige computeractiviteiten, zoals games of presentaties, vereiste een hoger reactievermogen en betere prestaties van het systeem zonder enige onderbrekingen.Wanneer uw laptop werkt op batterijvermogen, is het aanbevolen minder dringende bewerkingen die extra stroom zullen verbruiken, worden uitgesteld tot de laptop opnieuw op de netstroom is aangesloten.

Om zich aan deze specifieke situaties aan te passen, bevat Bitdefender Internet Security 2012 twee speciale gebruiksmodi:

- Spelmodus
- Laptop-modus

2.7.1. Spelmodus

De Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden.Als u in de Spelmodus bent, worden de volgende instellingen toegepast:

- Alle Bitdefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Auto scan is uitgeschakeld.Auto scan zoekt en gebruikt tijdsegmenten wanneer het gebruik van de systeembronnen daalt onder een bepaalde drempel om terugkerende scans van het volledige systeem uit te voeren.

- De Bitdefender-firewall is ingesteld op de normale modus (**Paranoïde-modus** is uitgeschakeld).Dit betekent dat alle nieuwe verbindingen (inkomend en uitgaand) automatisch zijn toegestaan, ongeacht de poort en het gebruikte protocol.
- Auto update is uitgeschakeld.
- De Bitdefender-werkbalk in uw webbrowser wordt uitgeschakeld wanneer u op browser gebaseerde online spelletjes speelt.

Als de Spelmodus is ingeschakeld, ziet u de letter G boven het  Bitdefender-pictogram.

Gebruik van de Spelmodus

Standaard gaat Bitdefender automatisch in de Spelmodus als u een spel start uit de lijst van Bitdefender's bekende spelen of als een applicatie overgaat op volledig scherm.Bitdefender zal automatisch terugkeren naar de normale gebruiksmodus wanneer u het spel afsluit of wanneer de gedetecteerde toepassing het volledig scherm afsluit.

Als u de Spelmodus handmatig wilt inschakelen, moet u een van de volgende methoden gebruiken:

- Rechtsklik op het Bitdefender pictogram in het systeemvak en selecteer **Spelmodus aanzetten**.
- Druk op `Ctrl+Shift+Alt+G` (de standaard sneltoets).

Belangrijk

Vergeet niet de Spelmodus uit te zetten als u klaar bent. Doe dit op dezelfde manier als bij het aanzetten.

De sneltoets voor de Spelmodus wijzigen

U kan de Spelmodus handmatig inschakelen met de standaard sneltoets `Ctrl+Alt+Shift+G`.Volg deze stappen als u de sneltoets wilt veranderen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Instellingen**.
4. Stel de gewenste sneltoets in onder de optie **Sneltoetsen Spelmodus inschakelen**:
   a. Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (`Ctrl`), Shift toets (`Shift`) of Alternate toets (`Alt`).
   b. Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

Bijvoorbeeld, als u de Ctrl+Alt+D sneltoets wilt gebruiken, kruist u Ctrl en Alt aan en typt u D.

Opmerking
Om de sneltoets uit te schakelen, schakelt u de optie **Sneltoetsen Spelmodus inschakelen** uit.

De automatische spelmodus in- of uitschakelen

Volg deze stappen om de automatische spelmodus in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Instellingen**.
4. Schakel de automatische spelmodus in of uit door op de overeenkomende schakelaar te klikken.

2.7.2. Laptop-modus

De Laptop-modus is speciaal bestemd voor laptop en notebook gebruikers. Het doel is dat Bitdefender een zo klein mogelijke invloed op het stroomverbruik heeft als deze apparaten op de accu werken.Wanneer Bitdefender werkt in de Laptop-modus, worden de functies Auto scan en Auto update uitgeschakeld omdat ze meer systeembronnen vereisen en hierdoor ook het stroomverbruik verhogen.

Bitdefender detecteert wanneer uw laptop overschakelt op accuvoeding en gaat automatisch in de Laptop-modus.Op dezelfde manier verlaat Bitdefender automatisch de Laptop-modus, als de laptop niet langer op de accu werkt.

Volg deze stappen om de automatische laptop-modus in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Instellingen**.
4. Schakel de automatische laptopmodus in of uit door op de overeenkomende schakelaar te klikken.

Als Bitdefender niet is geïnstalleerd op een laptop, moet u de automatische laptop-modus uitschakelen.

2.8. Wachtwoordbeveiligde Bitdefender-instellingen

Als u niet de enige persoon met beheermachtigingen bent die deze computer gebruikt, raden wij u aan uw Bitdefender-instellingen te beveiligen met een wachtwoord.

Volg de onderstaande stappen om de wachtwoordbeveiliging voor de instellingen van Bitdefender te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Instellingen**.
4. Schakel de wachtwoordbeveiliging in door in het onderdeel **Wachtwoordbeveiligde instellingen** op de schakelaar te klikken.
5. Klik op de koppeling **Wachtwoord wijzigen**.
6. Voer het wachtwoord in de twee velden in en klik op **OK**.Het wachtwoord moet minstens 8 tekens lang zijn.

Zodra u een wachtwoord hebt ingesteld, zal iedereen die de Bitdefender-instellingen probeert te wijzigen, eerst het wachtwoord moeten opgeven.

Belangrijk

Zorg dat u uw wachtwoord onthoudt of bewaar het op een veilige plaats.Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Volg deze stappen om de wachtwoordbeveiliging te verwijderen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Instellingen**.
4. Schakel de wachtwoordbeveiliging uit door in het onderdeel **Wachtwoordbeveiligde instellingen** op de schakelaar te klikken.
5. Voer het wachtwoord in en klik op **OK**.

2.9. Anonieme gebruiksrapporten

Standaard verzendt Bitdefender rapporten met informatie over uw gebruik van het programma naar de Bitdefender-servers.Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden.Merk op dat deze rapporten geen vertrouwelijke gegevens, zoals

uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

Volg deze stappen als u het verzenden van anonieme gebruiksrapporten wilt stopzetten:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Geavanceerd**.
4. Schakel anonieme gebruiksrapporten uit door op de overeenkomende schakelaar te klikken.

2.10. Bitdefender herstellen of verwijderen

Als u Bitdefender Internet Security 2012 wilt repareren of verwijderen, volgt u het pad vanaf het menu Start van Windows: **Start → Alle programma's → Bitdefender 2012 → Repareren of verwijderen**.

Selecteer de actie die u wilt uitvoeren:

- **Repareren** - alle programmacomponenten opnieuw installeren.
- **Verwijderen** - om alle geïnstalleerde componenten te verwijderen.

Opmerking
Wij raden u aan de optie **Verwijderen** te selecteren voor een zuivere nieuwe installatie.

Wacht tot Bitdefender de door u geselecteerde actie heeft voltooid.Dit zal enkele minuten duren.

U moet de computer opnieuw opstarten om het proces te voltooien.

3. Bitdefender-interface

Bitdefender Internet Security 2012 voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.

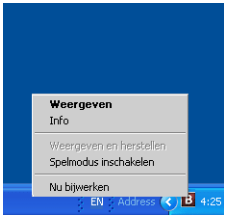
Om de status van het product te zien en essentiële taken uit t voeren, is het systeemvakpictogram van Bitdefender op elk ogenblik beschikbaar.

Het hoofdvenster biedt u snelle toegang tot de productmodules en belangrijke productinformatie en biedt u de mogelijkheid algemene taken uit te voeren.

Om uw Bitdefender-product gedetailleerd te configureren en geavanceerde beheertaken uit te voeren, kunt u alle benodigde hulpmiddelen terugvinden in het venster Instellingen.

3.1. Systeemvakpictogram

Om het volledige product sneller te beheren, kunt u het Bitdefender-pictogram in het systeemvak gebruiken.Wanneer u dubbelklikt op dit pictogram, wordt Bitdefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het Bitdefender-product snel kunt beheren.



Systeemvakpictogram

- **Weergeven** - opent het hoofdvenster van Bitdefender.
- **Info** - opent een venster waar u informatie over Bitdefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.
- **Alle problemen herstellen** - helpt u de huidige zwakke punten in de beveiliging te verwijderen.Als de optie niet beschikbaar is, moeten er geen problemen worden opgelost.Raadpleeg *"Problemen aan het oplossen"* (p. 11) voor meer gedetailleerde informatie.
- **Spelmodus in-/uitschakelen** - schakelt de Spelmodus in/uit.
- **Update nu** - start een directe update.U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van Bitdefender.

Het systeemvakpictogram van Bitdefender brengt u door middel van een speciaal pictogram op de hoogte van problemen die uw computer beïnvloeden of van de manier waarop het product werkt. Deze symbolen zijn de volgende:

Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

 Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem.U moet ze controleren en herstellen wanneer u tijd hebt.

 Het product werkt op Spelmodus.

 Bitdefender Auto Pilot is ingeschakeld.

Als Bitdefender niet werkt, verschijnt het systeemvakpictogram op een grijze achtergrond:  .Dit doet zich doorgaans voor wanneer de licentiesleutel vervalt. Dit kan ook optreden wanneer de Bitdefender-services niet reageren of wanneer andere fouten de normale werking van Bitdefender beïnvloeden.

3.2. Hoofdvenster

Via het hoofdvenster van Bitdefender kunt u algemene taken uitvoeren, snel beveiligingsproblemen oplossen, informatie over gebeurtenissen in het productgebruik weergeven en productinstellingen aanpassen.U kunt het allemaal met slechts enkele klikken op de knop.

Het venster is geordend in twee hoofdgebieden:

Werkbalk boven
: Hier kunt u de beveiligingsstatus van de computer controleren en krijgt u toegang tot belangrijke taken.

Panelengebied
: Hier kunt u de belangrijkste Bitdefender-modules beheren.

Daarnaast vindt u in het onderste deel van het venster verschillende nuttige koppelingen.

Koppeling	Beschrijving
Opmerkingen	Opent een webpagina in uw browser waar u een korte vragenlijst kunt invullen met betrekking tot uw ervaring bij het gebruik van het product.Wij baseren ons op uw feedback bij onze voortdurende inzet om de Bitdefender-producten te verbeteren.
Registratie voltooien / MyBitdefender	Opent het MyBitdefender-accountvenster waarin u een account kunt maken of kunt aanmelden bij een account.Een MyBitdefender-account is vereist voor het ontvangen van updates en te genieten van de online functies van uw product.Meer informatie over de manier waarop u een account kunt maken en kunt genieten van de voordelen hiervan, vindt u op “*Aanmelden bij MyBitdefender*” (p. 9).

Koppeling	Beschrijving
Informatie Licentie	Hiermee wordt een venster geopend waarin u informatie over de huidige licentiesleutel kunt zien en uw product kunt registreren met een nieuwe licentiesleutel.
Support	Klik op deze koppeling als u hulp nodig hebt bij Bitdefender.
	Voegt vraagtekens toe in verschillende gebieden van het Bitdefender-venster om u te helpen gemakkelijk informatie te vinden over de verschillende interface-elementen. Beweeg uw muiscursor over een markering om snelle informatie over het element ernaast te zien.

3.2.1. Werkbalk boven

De werkbalk bovenaan bevat de volgende elementen:

- **Het gebied Beveiligingsstatus** aan de linkerzijde van de werkbalk informeert u als er problemen zijn die de beveiliging van uw computer beïnvloeden en helpt u bij het oplossen van het probleem.

  De kleur van het gebied van de beveiligingsstatus verandert afhankelijk van de gedetecteerde problemen en er worden verschillende berichten weergegeven:

  - **Het gebied wordt groen gekleurd.** Er zijn geen problemen om op te lossen.Uw computer en gegevens zijn beveiligd.
  - **Het gebied wordt geel gekleurd.** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem.U moet ze controleren en herstellen wanneer u tijd hebt.
  - **Het gebied wordt rood gekleurd.** Kritieke problemen beïnvloeden de beveiliging van uw systeem.U moet deze problemen onmiddellijk aanpakken.

  Door te klikken op de knop **Problemen weergeven** in the midden van de werkbalk of op een willekeurige plaats in het gebied met de beveiligingsstatus aan de linkerzijde, krijgt u toegang tot een wizard waarmee u bedreigingen gemakkelijk van uw computer kunt verwijderen.Raadpleeg “*Problemen aan het oplossen*” (p. 11) voor meer gedetailleerde informatie.

- Met **Gebeurtenissen** krijgt u toegang tot een gedetailleerde geschiedenis van relevante gebeurtenissen die zich hebben voorgedaan tijdens de activiteiten van het product.Raadpleeg “*Gebeurtenissen*” (p. 13) voor meer gedetailleerde informatie.
- Met **Instellingen** krijgt u toegang tot het instellingsvenster waarin u de productinstellingen kunt configureren.Raadpleeg “*Venster Instellingen*” (p. 26) voor meer gedetailleerde informatie.

- Met **Auto pilot** kunt u de Auto pilot inschakelen en genieten van een volledig stille beveiliging.Raadpleeg “*Auto Pilot*” (p. 14) voor meer gedetailleerde informatie.

3.2.2. Panelengebied

In het panelengebied kunt u de Bitdefender-modules direct beheren.

U kunt de panelen ordenen zoals u dat wilt.Om het gebied opnieuw te ordenen volgens uw behoeften, sleept u de individuele panelen naar andere sleuven.

Om te bladeren door de panelen, gebruikt u de schuifregelaar onder het panelengebied of de pijlen aan de rechter- en linkerzijde.

Elke modulepaneel bevat de volgende elementen van boven naar beneden:

- De naam van de module.
- Een statusbericht.
- Het pictogram van de module.Klik op het pictogram van een module om zijn instellingen te configureren in het venster Instellingen.
- Een knop waarmee u belangrijke taken met betrekking tot de module kunt uitvoeren.
- Op bepaalde panelen is er een selectievakje beschikbaar waarmee u een belangrijke functie van de module kunt in- of uitschakelen.

De beschikbare panelen in dit gebied zijn:

Antivirus

Antivirusbescherming is de basis van uw beveiliging. Bitdefender beschermt u in real time en op aanvraag tegen elk type malware, zoals virussen, Trojaanse paarden, spyware, adware, enz.

Via het paneel Antivirus krijgt u gemakkelijk toegang tot de belangrijke scantaken.Klik op **Nu scannen** en selecteer een taak in het vervolgkeuzemenu.

- Quick Scan
- Volledige systeemscan
- Aangepast scannen
- Kwetsbaarheidsscan
- Helpmodus

Via de schakelaar **Auto scan** kunt u de functie Auto scan in- of uitschakelen.

Raadpleeg “*Antivirusbeveiliging*” (p. 39) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

Firewall

De firewall beschermt u terwijl u verbonden bent met netwerken en internet door alle verbindingspogingen te filteren.

Door in het paneel Firewall te klikken op **Netwerkdetails**, kunt u de instellingen voor de netwerkverbinding configureren.

Via het selectievakje Firewall kunt u de firewallbeveiliging in- of uitschakelen.

Waarschuwing

Omdat het uw computer blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn.Schakel de firewall zo snel mogelijk opnieuw in.

Meer informatie over de firewallconfiguratie, vindt u onder "*Firewall*" (p. 97).

Antispam

De Bitdefender-antispammodule zorgt ervoor dat uw Postvak IN vrij blijft van ongewenste e-mails door het POP3-mailverkeer te filteren.

Klik op **Beheren** in het paneel Antispam en selecteer Vrienden of Spammers in het vervolgkeuzemenu om de overeenkomende adressenlijst te bewerken.

Via het selectievakje Antispam kunt u de antispambeveiliging in- of uitschakelen.

Meer informatie over het configureren van de antispambeveiliging, vindt u onder "*Antispam*" (p. 64).

Update

In een wereld waar cybercriminelen voortdurend nieuwe manieren uitzoeken om schade te veroorzaken, is het van cruciaal belang uw beveiligingsoplossing up-to-date te houden om hen een stap voor te blijven.

Bitdefender is standaard ingesteld om elk uur te controleren op updates. Als u automatische updates wilt uitschakelen, kunt u de schakelaar **Auto Update** op het panel Update gebruiken.

Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij adviseren de automatische update zo kort mogelijk uit te schakelen. Als Bitdefender niet regelmatig wordt geüpdatet, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

Klik op het paneel **Nu bijwerken** om een onmiddellijke update te starten.

Meer informatie over het configureren van updates, vindt u onder "*Update*" (p. 111).

Ouderlijk Toezicht

Bitdefender Internet Security 2012 biedt een uitgebreid assortiment functies voor ouderlijk toezicht die u helpen het computergebruik van uw kinderen te beschermen en bewaken.

Klik op **Accounts beheren** in het paneel Ouderlijk toezicht om de instellingen te configureren voor de Windows-gebruikersaccounts op de computer.

Meer informatie over het configureren van Ouderlijk toezicht, vindt u onder "*Ouderlijk Toezicht*" (p. 82).

Privacybeheer

De module voor privacybeheer helpt u belangrijke persoonlijke gegevens privé te houden.Hiermee wordt u beschermd terwijl u met internet verbonden bent tegen phishingaanvallen, fraudepogingen, het lekken van persoonlijke gegevens, en meer.

Klik op de knop **Regels beheren** op het paneel Privacybeheer om naar de sectie Gegevensbeveiliging te gaan waar u de privacyregels kunt configureren.

Via het selectievakje Antiphishing kunt u de antiphishing-beveiliging in- of uitschakelen.

Meer informatie over het configureren van Bitdefender om uw privacy te beschermen, vindt u op "*Privacybeheer*" (p. 75).

Netwerk map

Met Netwerkmap kunt u de beveiliging van de computers bij u thuis probleemloos beheren vanaf één computer.

Om te starten, klikt u in het paneel Netwerkmap op **Beheren** en selecteert u **Netwerk inschakelen**.

Zodra het netwerk is ingeschakeld en op **Beheren** klikt u in het paneel Netwerkmap om toegang te krijgen tot de volgende opties.

- **Verbinding uitschakelen** - het netwerk uitschakelen.
- **Scan alles** - start een snelle scan of een volledige systeemscan op beheerde computers.
- **Alle computers bijwerken** - voer een update uit van de Bitdefender-producten op de beheerde computers.

Meer informatie vindt u onder "*Netwerk map*" (p. 107).

Safego

Om uw veiligheid op Facebook te verbeteren, kunt u Safego, de Bitdefender-beveiligingsoplossing voor sociale netwerken, direct vanaf uw product openen.

Klik op **Activeren** om Safego te activeren en te beheren vanaf uw Facebook-account.

Als u Safego al hebt geactiveerd, zult u de statistieken met betrekking tot zijn activiteiten kunnen openen door op de knop **Rapporten weergeven** te klikken.

Meer informatie vindt u onder "*Safego-beveiliging voor sociale netwerken*" (p. 115).

3.3. Venster Instellingen

Het instellingsvenster biedt u toegang tot elke component en de aanpassingsmogelijkheden van het product.Hier kunt u Bitdefender in detail configureren.

Aan de linkerzijde van het venster ziet u een menu met alle beveiligingsmodules.Elke module heeft een of meer tabbladen waarop u de overeenkomende beveiligingsinstellingen kunt configureren of beveiligings- of beheertaken kunt uitvoeren.In de volgende lijst vindt u een korte beschrijving van elke module.

Algemeen
: Hiermee kunt u de algemene productinstellingen, zoals het instellingswachtwoord, de spelmodus, de laptopmodus, de proxy-instellingen en de statuswaarschuwingen, configureren.

Antivirus
: Hiermee kunt u uw bescherming tegen malware configureren, kwetsbaarheid van uw systeem detecteren en oplossen, scanuitsluitingen instellen en bestanden in quarantaine beheren.

Antispam
: Hiermee kunt u uw Postvak IN spamvrij houden en de antispaminstellingen in detail configureren.

Ouderlijk Toezicht
: Hiermee kan u uw kinderen beschermen tegen ongepaste inhoud door uw eigen computertoegangsregels te gebruiken.

Privacybeheer
: Hiermee voorkomt u diefstal van data van uw computer en beschermt u uw privacy als u online bent.De beveiliging configureren voor uw webbrowser, IM-software, het beheren van uw gegevensbeveiliging, en meer.

Firewall
: Hiermee kunt u de algemene firewallinstellingen, firewallregels, inbraakdetectie en netwerkbewakingsactiviteiten configureren.

Netwerk map
: Hiermee kunt u de Bitdefender-producten die zijn geïnstalleerd op uw thuiscomputers beheren vanaf één enkele computer configureren en beheren.

Update
: Hiermee kan u informatie krijgen over de laatste updates, voor het updaten van het product en voor het configureren van de details van het updateproces.

Daarnaast vindt u in het onderste deel van het venster verschillende nuttige koppelingen.

Koppeling	Beschrijving
Opmerkingen	Opent een webpagina in uw browser waar u een korte vragenlijst kunt invullen met betrekking tot uw ervaring bij het gebruik van het product.Wij baseren ons op uw feedback bij onze voortdurende inzet om de Bitdefender-producten te verbeteren.
Registratie voltooien / MyBitdefender	Opent het MyBitdefender-accountvenster waarin u een account kunt maken of kunt aanmelden bij een account.Een MyBitdefender-account is vereist voor het ontvangen van updates en te genieten van de online functies van uw product.Meer informatie over de manier waarop u een account kunt maken en kunt genieten van de voordelen hiervan, vindt u op "*Aanmelden bij MyBitdefender*" (p. 9).
Informatie Licentie	Hiermee wordt een venster geopend waarin u informatie over de huidige licentiesleutel kunt zien en uw product kunt registreren met een nieuwe licentiesleutel.
Support	Klik op deze koppeling als u hulp nodig hebt bij Bitdefender.
	Voegt vraagtekens toe in verschillende gebieden van het Bitdefender-venster om u te helpen gemakkelijk informatie te vinden over de verschillende interface-elementen. Beweeg uw muiscursor over een markering om snelle informatie over het element ernaast te zien.

Om terug te keren naar het hoofdvenster, klikt u op de knop **Home** in de rechterbovenhoek van het venster.

4. Zo werkt het

Dit hoofdstuk biedt stapsgewijze instructies voor het configureren van algemeen gebruikte instellingen of voor het voltooien van algemene taken met Bitdefender.Sommige onderwerpen bevatten verwijzingen naar andere onderwerpen waar u gedetailleerde informatie kunt vinden.

4.1. Een evaluatieversie registreren

Als u een evaluatieversie hebt geïnstalleerd, kunt u deze slechts voor een beperkte periode gebruiken.Om Bitdefender verder te blijven gebruiken na het verlopen van de evaluatieperiode, moet u uw product registreren met een licentiesleutel en een MyBitdefender-account maken.

- Volg deze stappen om Bitdefender uit te schakelen:

  1. Open het Bitdefender-venster.

2. Klik onderaan in het venster op de koppeling **Informatie licentie**.Het registratievenster wordt weergegeven.
3. Voer de licentiesleutel in en klik op **Nu registreren**.

   Als u geen licentiesleutel hebt, klikt u op de koppeling die in het venster is voorzien om naar een webpagina te gaan waar u een sleutel kunt aanschaffen.
4. Wacht tot het registratieproces is voltooid en sluit het venster.

- Volg deze stappen om een MyBitdefender-account te maken:

1. Open het Bitdefender-venster.
2. Klik onderaan in het venster op de koppeling **Registratie voltooien**.Het accountvenster wordt weergegeven.
3. Selecteer de overeenkomende koppeling om een nieuwe account te maken.
4. Typ de vereiste informatie in de overeenkomende velden.De gegevens die u hier opgeeft blijven vertrouwelijk.

   Klik op **Verzenden**.
5. Controleer uw e-mail en volg de ontvangen instructies om de registratie te voltooien.

Opmerking
U kunt het bijgeleverde e-mailadres en wachtwoord gebruiken om u aan te melden bij uw account op http://my.bitdefender.com.

4.2. Hoe kan ik Bitdefender registreren zonder internetverbinding?

Als u net Bitdefender hebt aangeschaft en geen internetverbinding hebt, kunt u Bitdefender nog steeds offline registreren.

Volg deze stappen om Bitdefender te registreren met uw licentiesleutel:

1. Ga naar een pc die verbonden is met internet.U kunt bijvoorbeeld de computer van een vriend of een pc vanaf een openbare plaats gebruiken.
2. Ga naar https://my.bitdefender.com om een MyBitdefender-account te maken.
3. Meld u aan bij uw account en selecteer **Offline registratie verkrijgen**.
4. Voer de licentiesleutel in die u hebt aangeschaft.
5. Klik op **Verzenden** om een bevestigingscode te verkrijgen.

Belangrijk
Noteer de bevestigingscode.

6. Terugkeren naar uw pc met de bevestigingscode.
7. Open het Bitdefender-venster.
8. Klik onderaan in het venster op de koppeling **Informatie licentie**.Het registratievenster wordt weergegeven.
9. Selecteer de optie om het product te registreren met een bevestigingscode.
10. Voer de bevestigingscode in het overeenkomende veld in en klik op **Verzenden**.
11. Wacht tot het registratieproces is voltooid en klik op **Voltooien**.

4.3. Upgraden naar een ander Bitdefender 2012-product

U kunt probleemloos een upgrade uitvoeren van het ene Bitdefender 2011-product naar een ander product.

Laten we het volgende scenario overwegen: U hebt Bitdefender Internet Security 2012 een tijdje gebruikt en onlangs besloten om over te stappen naar Bitdefender Total Security 2012 en de extra functies die deze versie biedt.

U hoeft alleen een licentiesleutel aan te schaffen voor het Bitdefender 2012-product dat u wilt upgraden en dit in het registratievenster van het Bitdefender 2012-product dat u momenteel gebruikt, in te voeren.

Volg deze stappen:

1. Open het Bitdefender-venster.
2. Klik onderaan in het venster op de koppeling **Informatie licentie**.Het registratievenster wordt weergegeven.
3. Voer de licentiesleutel in en klik op **Nu registreren**.
4. Bitdefender zal u laten weten dat de licentiesleutel voor een ander product is en u de mogelijkheid bieden dit te installeren.Klik op de overeenkomende koppeling en volg de procedure om de upgrade uit te voeren.

4.4. Wanneer moet ik Bitdefender opnieuw installeren?

In sommige situaties zult u mogelijk uw Bitdefender-product opnieuw moeten installeren.

Typische situaties waarin u Bitdefender opnieuw moet installeren, zijn ondermeer de volgende:

- u hebt het besturingssysteem opnieuw geïnstalleerd.
- u hebt een nieuwe computer aangeschaft
- u wilt de weergavetaal van de Bitdefender-interface wijzigen

Om Bitdefender opnieuw te installeren, kunt u de installatieschijf gebruiken die u hebt aangeschaft of kunt u een nieuwe versie downloaden van de Bitdefender-website.

Tijdens de installatie wordt u gevraagd het product te registreren met uw licentiesleutel.

Als u uw licentiesleutel niet kunt vinden, kunt u zich aanmelden bij https://my.bitdefender.com om de sleutel op te halen.Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.

4.5. Wanneer verloopt mijn Bitdefender-bescherming?

Volg deze stappen om uit te zoeken hoeveel dagen uw licentiesleutel nog geldig is:

1. Open het Bitdefender-venster.
2. Klik onderaan in het venster op de koppeling **Informatie licentie**.
3. In het venster **Uw product registreren** ziet u het resterende aantal dagen.

4.6. Hoe kan ik mijn Bitdefender-beveiliging vernieuwen?

Wanneer de beveiliging van Bitdefender op het punt staat te vervallen, moet u uw licentiesleutel vernieuwen.

- Volg deze stappen om een website te bezoeken waar u uw Bitdefender-licentiesleutel kunt verlengen:
  1. Open het Bitdefender-venster.
  2. Klik onderaan in het venster op de koppeling **Informatie licentie**.
  3. Klik op **Geen licentiesleutel? Nu kopen.**
  4. Er wordt een webpagina geopend op uw webbrowser waar u een Bitdefender-licentiesleutel kunt aanschaffen.

  Opmerking
  Als alternatief kunt u contact opnemen met de kleinhandelaar bij wie u het Bitdefender-product hebt gekocht.

- Volg deze stappen om uw Bitdefender te registreren met de nieuwe licentiesleutel:
  1. Open het Bitdefender-venster.
  2. Klik onderaan in het venster op de koppeling **Informatie licentie**.Het registratievenster wordt weergegeven.
  3. Voer de licentiesleutel in en klik op **Nu registreren**.
  4. Wacht tot het registratieproces is voltooid en sluit het venster.

Voor meer informatie kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in sectie “*Ondersteuning*” (p. 140).

4.7. Welk Bitdefender-product gebruik ik?

Volg deze stappen om uit te zoeken welk Bitdefender-programma u hebt geïnstalleerd:

1. Open het Bitdefender-venster.
2. Bovenaan het venster zou u een van de volgende items moeten zien:
   - Bitdefender Antivirus Plus 2012
   - Bitdefender Internet Security 2012
   - Bitdefender Total Security 2012

4.8. Een bestand of map scannen

De eenvoudigste en aanbevolen manier om een bestand of map te scannen is klikken met de rechtermuisknop op het object dat u wilt scannen en de optie **Scannen met Bitdefender** te selecteren in het menu.Volg de Antivirusscanwizard om de scan te voltooien.

Typische situaties voor het gebruik van deze scanmethode zijn ondermeer de volgende:

- U vermoedt dat een specifiek bestand of een specifieke map geïnfecteerd is.
- Wanneer u bestanden waarvan u denkt dat ze mogelijk gevaarlijk zijn, downloadt van internet.
- Scan een netwerkshare voordat u bestanden naar uw computer kopieert.

4.9. Hoe kan ik mijn systeem scannen?

Volg deze stappen om een volledige scan op het systeem uit te voeren:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.
3. Klik op **Nu scannen** en selecteer **Volledige systeemscan** in het vervolgkeuzemenu.
4. Volg de Antivirusscanwizard om de scan te voltooien.

4.10. Een aangepaste scantaak maken

Ga als volgt te werk om een aangepaste scantaak te maken:

1. Open het Bitdefender-venster.

2. Ga naar het deelvenster **Antivirus**.
3. Klik op **Nu scannen** en selecteer **Aangepaste scan** in het vervolgkeuzemenu.
4. Klik op **Doel toevoegen** om de te scannen bestanden of mappen te selecteren.
5. Klik op **Scanopties** als u de scanopties in detail wilt configureren.

   U kunt de optie **Computer uitschakelen** selecteren.

   Als er tijdens het scannen geen bedreigingen zijn, wordt uw computer uitgeschakeld wanneer de scan voltooid is.Denk eraan dat dit, telkens wanneer u deze taak uitvoert, het standaard gedrag zal zijn.
6. Klik op **Scannen starten** om de taak uit te voeren.

4.11. Een map uitsluiten van de scan

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen.

Uitsluitingen zijn bedoeld voor gebruikers met een gevorderde computerkennis en alleen in de volgende situaties:

- U hebt een grote map op uw systeem waarin u films en muziek bewaart.
- U hebt een groot archief op uw systeem waarin u verschillende gegevens bewaart.
- U bewaart een map waarin u verschillende types software en toepassingen installeert voor testdoeleinden.Het scannen van de map kan resulteren in het verlies van bepaalde gegevens.

Volg deze stappen om de map toe te voegen aan de lijst Uitsluitingen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Klik op de koppeling **Uitgesloten bestanden en mappen**.
5. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
6. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**.
7. Klik op **Toevoegen** en klik vervolgens op **OK** om de wijzigingen op te slaan en het venster te sluiten.

4.12. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt?

Er zijn gevallen waarbijBitdefender een rechtmatig bestand verkeerdelijk markeert als een bedreiging (vals positief).Om deze fout te corrigeren, voegt u het bestand toe aan het gebied Uitsluitingen van Bitdefender:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Open het Bitdefender-venster.
   b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
   c. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
   d. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
2. Verborgen objecten weergeven in Windows.Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 150) voor meer informatie hierover.
3. Het bestand herstellen vanaf het quarantainegebied:
   a. Open het Bitdefender-venster.
   b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
   c. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Quarantaine**.
   d. Selecteer het bestand en klik op **Herstel**.
4. Het bestand toevoegen aan de lijst Uitsluitingen.Raadpleeg "*Een map uitsluiten van de scan*" (p. 33) voor meer informatie hierover.
5. Schakel de real time antivirusbeveiliging van Bitdefender in.
6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectiehandtekening kunnen verwijderen.Raadpleeg "*Hulp vragen*" (p. 141) voor meer informatie hierover.

4.13. Windows-gebruikersaccounts maken

Een Windows-gebruikersaccount is een uniek profiel dat alle instellingen, privileges en persoonlijke bestanden voor elke gebruiker bevat.Via de Windows-accounts kan de beheerder van de thuis-pc de toegang voor elke gebruiker beheren.

Het instellen van gebruikersaccounts is handig wanneer de pc zowel door ouders als door kinderen wordt gebruikt. Ouders kunnen accounts instellen voor elk kind.

Selecteer uw besturingssysteem voor meer informatie over het maken van Windows-accounts.

- Windows XP:

1. Meld u als beheerder aan op uw computer.
2. Klik op Start, Configuratiescherm en daarna op Gebruikersaccounts.
3. Klik op Een nieuwe account maken.
4. Voer de naam in voor de gebruiker. U kunt de volledige naam, de voornaam of een bijnaam van de persoon gebruiken. Klik daarna op Volgende.
5. Kies voor het accounttype de optie Beperkt en vervolgens Account maken. Beperkte accounts zijn geschikt voor kinderen omdat ze dan geen wijzigingen aan het systeem kunnen aanbrengen of bepaalde toepassingen kunnen installeren.
6. Uw nieuwe account wordt gemaakt en weergegeven in het scherm Accounts beheren.

- Windows Vista of Windows 7:

1. Meld u als beheerder aan op uw computer.
2. Klik op Start, Configuratiescherm en daarna op Gebruikersaccounts.
3. Klik op Een nieuwe account maken.
4. Voer de naam in voor de gebruiker. U kunt de volledige naam, de voornaam of een bijnaam van de persoon gebruiken. Klik daarna op Volgende.
5. Klik voor het accounttype op Standaard en vervolgens op Account maken. Beperkte accounts zijn geschikt voor kinderen omdat ze dan geen wijzigingen aan het systeem kunnen aanbrengen of bepaalde toepassingen kunnen installeren.
6. Uw nieuwe account wordt gemaakt en weergegeven in het scherm Accounts beheren.

Opmerking

Nu u nieuwe gebruikersaccounts hebt toegevoegd, kunt u wachtwoorden maken voor de accounts.

4.14. Mijn kinderen beschermen tegen online bedreigingen

Met Ouderlijk toezicht van Bitdefender kunt u de toegang tot internet en specifieke toepassingen beperken en voorkomen dat uw kinderen ongepaste inhoud bekijken wanneer u niet in de buurt bent.

U kan Ouderlijk Toezicht configureren voor het blokkeren van:

- ongeschikte webpagina's.
- Toegang tot het Internet gedurende een bepaalde periode (bijvoorbeeld als het tijd is om huiswerk te maken).
- webpagina's, e-mailberichten en instant messages die bepaalde sleutelwoorden bevatten.

- toepassingen zoals spelletjes, chat, programma's voor het delen van bestanden en dergelijke.
- instant messages van andere dan de toegelaten IM contacten.

Volg deze stappen om Ouderlijk toezicht te configureren:

1. Creëer beperkte (standaard) Windows gebruikersaccounts voor uw kinderen.Meer informatie vindt u onder "*Windows-gebruikersaccounts maken*" (p. 34).
2. Zorg dat u bij de computer bent aangemeld met een beheerdersaccount.Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.
3. Configureer Ouderlijk Toezicht voor de Windows gebruikersaccounts van uw kinderen.
   a. Open het Bitdefender-venster.
   b. Ga naar het deelvenster **Ouderlijk toezicht**.
   c. Klik op **Accounts beheren** en controleer of Ouderlijk toezicht is ingeschakeld voor de gebruikersaccount van uw kind.
   d. Stel de leeftijd van uw kind in door te klikken in het vak dat overeenkomt met de optie **Leeftijd**.Wanneer u de leeftijd van het kind instelt, worden de instellingen die voor die leeftijdscategorie als geschikt worden beschouwd, automatisch geladen volgens de ontwikkelingsnormen van het kind.
   e. Klik op **Instellingen** als u de instellingen voor Ouderlijk toezicht in detail wilt configureren.

Meer gedetailleerde informatie over het gebruik van Ouderlijk toezicht, vindt u onder "*Ouderlijk Toezicht*" (p. 82).

4.15. De blokkering opheffen van een website die door Ouderlijk toezicht is geblokkeerd

Met Bitdefender Ouderlijk toezicht hebt u het beheer over de inhoud waarvoor uw kinderen toegang hebben wanneer ze de computer gebruiken.

Als u de leeftijdscategorie voor uw kind instelt in Ouderlijk toezicht en slechts één Windows-account gebruikt, zult u geen toegang krijgen tot websites die geclassificeerd zijn als ongeschikt voor de geselecteerde leeftijdscategorie.

Als Ouderlijk toezicht de toegang tot een website blokkeert, kunt u een regel maken om de toegang tot die website expliciet toe te laten.

Volg deze stappen om de toegang tot een website toe te staan:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Ouderlijk toezicht**.

3. Klik op **Accounts beheren**.
4. Klik op de knop **Instellingen** om de gebruikersinstellingen te configureren.
5. Klik op **Website toestaan**.
6. Voer het websiteadres in het veld **Website** in.
7. Selecteer de gewenste actie voor deze regel - **Toestaan** en klik op **Voltooien** om de regel toe te voegen.
8. Open uw browser en ga naar de website.

4.16. Uw persoonlijke informatie beschermen

Privacybeheer bewaakt de gegevens die uw computer verlaten via webformulieren, e-mailberichten en expresberichten.

Om zeker te zijn dat er geen persoonlijke gegevens uw computer verlaten zonder uw toestemming, moet u de geschikte gegevensbeveiligingsregels en uitzondering op deze regels maken.

De regels voor de gegevensbeveiliging vermelden de informatie die moet worden geblokkeerd.

Volg deze stappen om een regel voor Gegevensbeveiliging te maken:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Privacybeheer** en klik vervolgens op het tabblad **Gegevensbeveiliging**.
4. Als **Gegevensbeveiliging** is uitgeschakeld, schakelt u dit in met de overeenkomende schakelaar.
5. Selecteer de optie **Regel toevoegen** om de wizard Gegevensbeveiliging te starten.
6. Volg de stappen van de wizard.

4.17. Bitdefender configureren voor het gebruik van een proxy-internetverbinding

Als uw computer een internetverbinding maakt via een proxyserver, moet u Bitdefender configureren met de proxy-instellingen.Bitdefender zal standaard de proxy-instellingen van uw systeem automatisch detecteren en importeren.

Belangrijk

Internetverbindingen bij u thuis gebruiken doorgaans geen proxyserver.Als vuistregel is het aanbevolen de proxyverbindingsinstellingen van uw Bitdefender-programma

te controleren en te configureren wanneer de updates niet werken.Als Bitdefender een update kan uitvoeren, dan is de toepassing correct geconfigureerd voor het maken van een internetverbinding.

Volg de onderstaande stappen om de proxy-instellingen te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Algemeen** en klik vervolgens op het tabblad **Geavanceerd**.
4. Schakel het proxy-gebruik in door in het onderdeel **Proxy-instellingen** op de schakelaar te klikken.
5. Klik op de koppeling **Proxy's beheren**.
6. Er zijn twee opties voor het instellen van de proxy-instellingen:
   - **Proxy-instellingen van de standaardbrowser importeren** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaardbrowser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

     Opmerking
     Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van Internet Explorer, Mozilla Firefox en Opera.

   - **Proxy-instellingen aanpassen** - proxy-instellingen die u zelf kunt configureren.U moet de volgende instellingen definiëren:
     - **Adres** - voer het IP-adres van de proxyserver in.
     - **Poort** - voer de poort in die Bitdefender gebruikt om een verbinding te maken met de proxyserver.
     - **Gebruikersnaam** - typ een gebruikersnaam die door de proxy wordt herkend.
     - **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Bitdefender gebruikt de beschikbare proxy-instellingen tot er een internetverbinding kan worden gemaakt.

Belangrijk
Denk eraan het proxy-gebruik uit te schakelen wanneer u schakelt naar een directe internetverbinding.

5. Antivirusbeveiliging

Bitdefender beveiligt uw computer tegen alle types malware (virussen, Trojanen, spyware, rootkits, enz.).De Bitdefender-bescherming is ingedeeld in twee categorieën:

- Scannen bij toegang - verhindert dat nieuwe malware-bedreigingen uw systeem binnenkomen.Bitdefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

  Met Scannen bij toegang bent u zeker van bescherming in real time tegen malware, een essentieel onderdeel van elk computerbeveiligingsprogramma.

  Belangrijk
  Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat virussen uw computer infecteren.

- Scannen op aanvraag - hiermee kan u malware die al op uw systeem aanwezig is, detecteren en verwijderen.Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat Bitdefender moet scannen, en Bitdefender doet dat - op aanvraag.

  Wanneer Auto scan is ingeschakeld, is het zelden nodig malwarescans handmatig uit te voeren.Auto Scan zal uw computer voortdurend opnieuw scannen en de geschikte acties ondernemen wanneer er malware is gedetecteerd.Auto scan werkt alleen wanneer er voldoende systeembronnen beschikbaar zijn, zodat de computer niet wordt vertraagd.

Bitdefender scant automatisch alle verwisselbare media die op de computer zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend.Meer informatie vindt u onder “*Automatisch scannen van verwisselbare media*” (p. 52).

Geavanceerde gebruikers kunnen scanuitsluitingen configureren als ze niet willen dat er specifieke bestanden of bestandstypes worden gescand.Meer informatie vindt u onder “*Scanuitsluitingen configureren*” (p. 54).

Wanneer een virus of andere malware wordt gedetecteerd, zal Bitdefender automatisch proberen de malwarecode te verwijderen uit het geïnfecteerde bestand en het originele bestand reconstrueren.Deze bewerking wordt een desinfectie genoemd.Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen.Meer informatie vindt u onder “*Bestanden in quarantaine beheren*” (p. 57).

Als uw computer werd geïnfecteerd door malware, moet u “*Malware van uw systeem verwijderen*” (p. 131) raadplegen.Om u te helpen bij het opruimen van de malware die niet kan worden verwijderd van het Windows-besturingssysteem op uw computer, biedt Bitdefender u de Helpmodus.Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van malware, waarmee u uw computer onafhankelijk van

Windows kunt opstarten.Wanneer de computer start in de Helpmodus, is de Windows-malware inactief zodat deze gemakkelijk kan worden verwijderd.

Om u te beschermen tegen onbekende boosaardige toepassingen, gebruikt Bitdefender Actief virusbeheer, een geavanceerde heuristische technologie die de toepassingen die op uw systeem worden uitgevoerd, doorlopend bewaakt.Actief virusbeheer blokkeert automatisch toepassingen die een malware-achtig gedrag vertonen om te voorkomen dat ze uw computer beschadigen.In sommige gevallen kunnen rechtmatige toepassingen worden geblokkeerd. In dergelijke situaties kunt u Actief virusbeheer configureren om die toepassingen niet opnieuw te blokkeren door uitsluitingsregels te maken.Raadpleeg “*Actief virusbeheer*” (p. 58) voor meer informatie.

Heel wat vormen van malware zijn ontwikkeld voor het infecteren van systemen door gebruik te maken van hun kwetsbaarheden, zoals ontbrekende updates van besturingssystemen of verouderde toepassingen.Bitdefender helpt u bij de systeemkwetsbaarheden gemakkelijk te identificeren en op te lossen om uw computer veiliger te stellen tegen malware en hackers.Meer informatie vindt u onder “*Systeemkwetsbaarheden oplossen*” (p. 60).

5.1. Scannen bij toegang (real time-beveiliging)

Bitdefender geeft continu, real-time bescherming tegen een groot aantal types malware-bedreigingen door alle geopende bestanden, e-mailbestanden en communicatie via toepassingen voor instant messaging (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) te scannen.

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties.U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen.Als u een geavanceerde gebruiker bent, kunt u de scaninstellingen in detail configureren door een aangepast beveiligingsniveau te maken.

5.1.1. Malware die door Scannen bij toegang is gedetecteerd, controleren

Volg deze stappen om de malware die door Scannen bij toegang is gedetecteerd, te controleren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Virusscans**.Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.

4. Klik op een gebeurtenis om details erover weer te geven.

5.1.2. Het real time-beveiligingsniveau aanpassen

Het real time-beveiligingsniveau definieert de scaninstellingen voor real time-beveiliging.U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen.

Volg deze stappen om de standaard real time-beveiligingsinstellingen te herstellen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Sleep de schuifregelaar langs de schaal om het gewenste beveiligingsniveau in te stellen.Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

5.1.3. Een aangepast beveiligingsniveau maken

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden.U kunt de instellingen voor de real time-beveiliging in detail configureren door een aangepast beschermingsniveau te maken.

Volg deze stappen om een aangepast beveiligingsniveau te maken:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Klik op **Aangepast**.
5. Configureer de scaninstellingen zoals dat nodig is.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de woordenlijst.U kunt ook nuttige informatie vinden door op het internet te zoeken.
- **Scanopties voor geopende bestanden.** U kunt Bitdefender instellen om alleen alle geopende bestanden of toepassingen (programmabestanden) te scannen.Het scannen van alle geopende bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt voor betere systeemprestaties.

Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen.Deze categorie bevat de volgende bestandsextensies:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Binnen archieven scannen.** Het scannen binnenin de archieven verloopt langzaam en is een veeleisend proces, waardoor het niet aanbevolen is voor de real time-beveiliging.Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem.De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

  Als u beslist deze optie te gebruiken, kunt u een maximaal geaccepteerde groottelimiet instellen voor archieven die bij toegang moeten worden gescand.Schakel het overeenkomende selectievakje in en typ de maximale archiefgrootte (in MB).

- **Scanopties voor verkeer via e-mail, web en expresberichten.** Om te verhinderen dat er malware wordt gedownload naar uw computer, scant Bitdefender automatische de volgende ingangspunten van malware:
  - binnenkomende en uitgaande e-mails
  - webverkeer
  - bestanden ontvangen via Yahoo! Messenger en Windows Live Messenger

  Het scannen van het webverkeer kan het surfen op het weg iets vertragen, maar het zal malware blokkeren die afkomstig is van internet, inclusief downloads tijdens het passeren.

  Hoewel dit niet aanbevolen is, kunt u de antivirusscan van e-mails, internet of expresberichten uitschakelen om de systeemprestaties te verbeteren.Als u de overeenkomende scanopties uitschakelt, worden de e-mails en bestanden die

zijn ontvangen of gedownload via internet niet gescand, waardoor geïnfecteerde bestanden op uw computer moeten worden opgeslagen.Dit is geen belangrijke bedreiging omdat de real time-beveiliging de malware zal blokkeren wanneer u probeert toegang te krijgen tot de geïnfecteerde bestanden (openen, verplaatsen, kopiëren of uitvoeren).

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen.Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten.Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kun starten en geen toegang meer hebt tot uw gegevens.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.

5.1.4. De standaardinstellingen herstellen

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties.

Volg deze stappen om de standaard real time-beveiligingsinstellingen te herstellen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Klik op **Standaard**.

5.1.5. De real time-beveiliging in- of uitschakelen

Volg deze stappen om real time malwarebeveiliging in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Klik op de schakelaar om Scannen bij toegang in of uit te schakelen.
5. Als u de real time-beveiliging wilt uitschakelen, verschijnt een waarschuwingsvenster.U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen malware-bedreigingen.

5.1.6. Acties die worden ondernomen op gedetecteerde malware

Bestanden die door de real time-beveiliging zijn gedetecteerd, worden gegroepeerd in twee categorieën.

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een malwarehandtekening in de database van malwarehandtekeningen van Bitdefender.Bitdefender kan normaal de malwarecode van een geïnfecteerd bestand verwijderen en het originele bestand reconstrueren. Deze bewerking wordt een desinfectie genoemd.

Opmerking
Malwarehandtekeningen zijn fragmenten van codes die uit echte malwaremonsters zijn gehaald. Ze worden gebruikt door antivirusprogramma's voor het uitvoeren van patroonafstemming en het detecteren van malware.
De database met malwarehandtekeningen van Bitdefender is een verzameling van malwarehandtekeningen die elk uur wordt bijgewerkt door de malwareonderzoekers van Bitdefender.

- **Verdachte bestanden.** De bestanden worden gedetecteerd als verdacht door de heuristische analyse.Omdat B-HAVE een heuristische analysetechnologie is, kan Bitdefender niet zeker zijn of het bestand ook daadwerkelijk is geïnfecteerd met malware.Verdachte bestanden kunnen niet worden gedesinfecteerd omdat er geen desinfectieroutine beschikbaar is.

De volgende acties worden, afhankelijk van het type gedetecteerd bestand, automatisch ondernomen:

- Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren.Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Belangrijk
Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- Als een verdacht bestand wordt gedetecteerd, wordt het verplaatst naar de quarantaine om mogelijke infectie te voorkomen.

  Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender.Als

de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

5.2. Scannen op aanvraag

Bitdefender heeft als hoofddoel uw computer vrij te houden van virussen. Dit wordt in de eerste plaats gedaan door nieuwe virussen uit uw computer weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een virus zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder goed idee uw computer meteen te scannen op aanwezige virussen nadat u Bitdefender hebt geïnstalleerd. En het is zeker ook een goed idee om uw computer frequent te scannen op virussen.

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand.U kunt de computer scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren.Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

5.2.1. Auto Scan

Auto scan is een lichte scan op aanvraag die op de achtergrond al uw gegevens scant op malware en de geschikte acties onderneemt voor eventuele opgespoorde infecties.Auto scan zoekt en gebruikt tijdsegmenten wanneer het gebruik van de systeembronnen daalt onder een bepaalde drempel om terugkerende scans van het volledige systeem uit te voeren.

Voordelen van het gebruik van Auto scan.

- Dit heeft nagenoeg geen invloed op het systeem.
- Door de volledige harde schijf vooraf te scannen, worden toekomstige taken op aanvraag bijzonder snel.
- Scannen bij toegang zal eveneens veel minder tijd in beslag nemen.

Volg deze stappen om Auto scan in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.
3. Klik op de schakelaar om Auto scan in of uit te schakelen.

5.2.2. Een bestand of map scannen op malware

U moet bestanden en mappen scannen wanneer u vermoedt dat ze geïnfecteerd zijn.Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en

selecteer **Scannen met Bitdefender**.De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces.

5.2.3. Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om malware die op uw pc wordt uitgevoerd, te detecteren.Het uitvoeren van een Snelle scan duur doorgaans minder dan één minuut en gebruikt slechts een fractie van de systeembronnen die nodig zijn door een regelmatige virusscan.

Volg deze stappen om een Snelle scan uit te voeren:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.
3. Klik op **Nu scannen** en selecteer **Snelle scan** in het vervolgkeuzemenu.
4. Volg de Antivirusscanwizard om de scan te voltooien.

5.2.4. Een volledige systeemscan uitvoeren

De Volledige systeemscan scant de volledige computer op alle types malware die de beveiliging bedreigen, zoals virussen, spyware, adware, rootkits en andere.Als u Auto scan hebt uitgeschakeld, is het aanbevolen minstens een keer per weeg een volledige systeemscan uit te voeren.

Opmerking

Het scannen kan enige tijd duren omdat **Volledige systeemscan** een grondige scan van het volledige systeem uitvoert. Het is daarom aanbevolen deze taak uit te voeren wanneer u de computer niet gebruikt.

Voordat u een Volledige systeemscan uitvoert, wordt het volgende aanbevolen:

- Controleer of de malwarehandtekeningen van Bitdefender up-to-date zijn. Het scannen van uw computer met een oude handtekeningendatabase kan verhinderen dat Bitdefender nieuwe malware die sinds de laatste update is gevonden, detecteert.Meer informatie vindt u onder “*Update*” (p. 111).
- Alle open programma’s afsluiten

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.Meer informatie vindt u onder “*Een aangepaste scan configureren en uitvoeren*” (p. 47).

Volg deze stappen om een Volledige systeemscan uit te voeren:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.

3. Klik op **Nu scannen** en selecteer **Volledige systeemscan** in het vervolgkeuzemenu.
4. Volg de Antivirusscanwizard om de scan te voltooien.

5.2.5. Een aangepaste scan configureren en uitvoeren

Volg deze stappen om het scannen op malware gedetailleerd te configureren en uit te voeren:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.
3. Klik op **Nu scannen** en selecteer **Aangepaste scan** in het vervolgkeuzemenu.
4. Klik op **Doel toevoegen**, schakel de selectievakjes in die overeenkomen met de locatie die u wilt scannen op malware en klik vervolgens op **OK**.
5. Klik op **Scanopties** als u de scanopties wilt configureren.Een nieuw venster wordt weergegeven.Volg deze stappen:
   a. U kunt de scanopties gemakkelijk configureren door het scanniveau aan te passen. Sleep de schuifregelaar langs de schaal om het gewenste scanniveau in te stellen.Gebruik de beschrijving aan de rechterzijde van de schaal om het scanniveau te identificeren dat beter beantwoordt aan uw behoeften.

      Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden.Klik op **Aangepast** om de scanopties in detail te configureren. Aan het einde van dit gedeelte vindt u informatie over deze opties.

   b. Standaard probeert Bitdefender de malwarecode te verwijderen uit geïnfecteerde bestanden of, als de desinfectie mislukt, ze naar quarantaine te verplaatsen.Als de beide acties mislukken, wordt u gevraagd welke actie moet worden genomen voor de niet-opgeloste bedreigingen.

      Als u alleen malware wilt detecteren, zonder enige andere actie te ondernemen, schakelt u het overeenkomende selectievakje in het deel **Acties** in.

   c. U kunt ook deze algemene opties configureren:

      - **De taak uitvoeren met lage prioriteit.** Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
      - **Scanwizard minimaliseren naar systeemvak.** Minimaliseert het scanvenster naar het systeemvak. Dubbelklik op het pictogram Bitdefender om het programma te openen.
      - Geef de actie op die moet worden ondernomen als er geen bedreigingen zijn gevonden.

d. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

6. Klik op **Scannen starten** en volg de Antivirusscanwizard om het scannen te voltooien.Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de woordenlijst.U kunt ook nuttige informatie vinden door op het internet te zoeken.
- **Bestanden scannen.** U kunt Bitdefender instellen om alleen alle types bestanden of toepassingen (programmabestanden) te scannen.Het scannen van alle bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt om een snellere scan uit te voeren.

  Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen.Deze categorie bevat de volgende bestandsextensies: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scanopties voor archieven.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem.De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.Het is echter aanbevolen deze optie te gebruiken om eventuele potentiële bedreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke bedreiging gaat.

Opmerking
Het scannen van de gearchiveerde bestanden verlengt de algemene scanduur en vereist meer systeembronnen.

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen.Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten.Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kun starten en geen toegang meer hebt tot uw gegevens.
- **Geheugen scannen.** Selecteer deze optie om programma's te scannen die worden uitgevoerd in uw systeemgeheugen.
- **Register scannen.** Selecteer deze optie voor het scannen van registersleutels.Het Windows-register is een database die de configuratie-instellingen en opties opslaat voor de componenten van het Windows-besturingssysteem, evenals voor geïnstalleerde toepassingen.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw computers zijn opgeslagen.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Commerciële keyloggers negeren.** Selecteer deze opties als u commerciële keylogger-software op uw computer hebt geïnstalleerd en deze software gebruikt.Commerciële keyloggers zijn rechtmatige computerbewakingsprogramma's waarvan de basisfunctie eruit bestaat alles wat op het toetsenbord wordt getypt, te registreren.

5.2.6. Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map en selecteer **Scannen met Bitdefender**), verschijnt de Antivirusscanwizard van Bitdefender.Volg de wizard om het scannen te voltooien.

Opmerking
Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond.Zoek het pictogram voor de scanvoortgang in het systeemvak.U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Stap 1 – Scanlocaties kiezen

Deze stap verschijnt alleen wanneer u Aangepaste scan gebruikt.Meer informatie vindt u onder “*Een aangepaste scan configureren en uitvoeren*” (p. 47).

Stap 2 - Scan uitvoeren

Bitdefender start het scannen van de geselecteerde objecten.

U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

Wacht tot Bitdefender het scannen beëindigt.

Opmerking
Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

Wachtwoordbeveiligde archieven. Wanneer een met een wachtwoord beschermd archief wordt gedetecteerd, kunt u afhankelijk van de scaninstellingen worden gevraagd het wachtwoord op te geven.Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft.De volgende opties zijn beschikbaar:

- **Wachtwoord invoeren.** Als u wilt dat Bitdefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren.Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Alle wachtwoordbeveiligde items overslaan zonder ze te scannen.** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven.Bitdefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Klik op **OK** om door te gaan met scannen.

De scan stoppen of pauzeren. U kunt het scannen op elkogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard.Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

Stap 3 – Acties kiezen

Wanneer het scannen is voltooid, verschijnt een nieuw venster waarin u de scanresultaten kunt zien.

Klik op **Doorgaan** als er geen niet-opgeloste bedreigingen meer zijn.Anders moet u nieuwe acties configureren die moeten worden ondernomen op de niet-opgeloste bedreigingen om uw systeem te beschermen.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de malware waarmee ze zijn geïnfecteerd.Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kan een algemene actie selecteren die moet worden genomen voor alle groepen problemen of u kan afzonderlijke acties voor elke groep problemen selecteren.Een of meerdere van de volgende opties kunnen in het menu verschijnen.

Geen actie nemen
Er wordt geen actie ondernomen voor de geïnfecteerde bestanden.Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.

Desinfecteren
Verwijdert de malwarecode uit geïnfecteerde bestanden.

Wissen
Verwijdert gedetecteerde bestanden van de schijf.

Naar quarantaine
Verplaatst gedetecteerde bestanden naar de quarantaine.In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.Meer informatie vindt u onder *"Bestanden in quarantaine beheren"* (p. 57).

Bestand wijzigen
Wijzigt de naam van verborgen bestanden door `.bd.ren` toe te voegen aan hun naam.Hierdoor zult u dergelijke bestanden op uw computer kunnen zoeken en vinden, als die er zijn.

Houd ermee rekening dat deze verborgen bestanden geen bestanden zijn die u opzettelijk verbergt voor Windows. Het zijn de bestanden die worden verborgen door speciale programma's, bekend als rootkits.Rootkits zijn in wezen niet kwaadaardig. Ze worden echter algemeen gebruikt om ervoor te zorgen dat virussen en spyware niet detecteerbaar zijn voor normale antivirusprogramma's.

Klik op **Doorgaan** om de aangegeven acties toe te passen.

Stap 4 – Overzicht

Wanneer Bitdefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster.Als u uitgebreide informatie over het scanproces wenst, klikt u op **Logboek weergeven** om het scanlogboek weer te geven.

Belangrijk
Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien.

Klik op **Sluiten** om het venster te sluiten.

Bitdefender kon bepaalde problemen niet oplossen

In de meeste gevallen desinfecteert Bitdefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie.Er zijn echter problemen die niet automatisch kunnen worden opgelost.Meer informatie en instructies over het handmatig verwijderen van malware, vindt u onder *"Malware van uw systeem verwijderen"* (p. 131).

Bitdefender detecteerde verdachte bestanden

Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse als potentieel geïnfecteerd met malware waarvan de signatuur nog niet bekend is.

Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het Bitdefender Lab te sturen.Klik op **OK** om deze bestanden naar het Bitdefender laboratorium te verzenden voor verdere analyse.

5.2.7. Scanlogboeken controleren

Telkens wanneer u een scan uitvoert, wordt een scanlogboek gemaakt.Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **Logboek weergeven** te klikken.

Volg deze stappen om de scanlogboeken op een later tijdstip te controleren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Virusscans**.Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
4. In de gebeurtenissenlijst kunt u controleren welke scans onlangs werden uitgevoerd.Klik op een gebeurtenis om details erover weer te geven.
5. Klik op **Logboek weergeven** om het scanlogboek te openen.Het scanlog wordt geopend in uw standaard webbrowser.

5.3. Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw computer en scant dit op de achtergrond.Dit is aanbevolen om infecties van uw computer door virussen en andere malware te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

- Cd's/dvd's
- USB-opslagapparaten, zoals flashpennen en externe harde schijven
- toegewezen (externe) netwerkstations

U kunt het automatisch scannen afzonderlijk configureren voor elke categorie opslagapparaten.Automatisch scannen van toegewezen netwerkstations is standaard uitgeschakeld.

5.3.1. Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, start het programma met scannen op malware op de achtergrond (op voorwaarde dat de automatische scan is ingeschakeld voor dat type apparaat).Een Bitdefender-scanpictogram verschijnt in het systeemvak.U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Als Auto Pilot is ingeschakeld, wordt u niet gehinderd door herinnering aan de scan.De scan wordt alleen geregistreerd en de informatie over de scan zal beschikbaar zijn in het venster Gebeurtenissen.

Als Auto Pilot is uitgeschakeld:

1. U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.
2. Wanneer tijdens de scan een door een wachtwoord beschermd archief wordt gedetecteerd, kunt u worden gevraagd het wachtwoord op te geven.Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft.U kunt kiezen om het wachtwoord in te voeren, het bestand overslaan voor het scannen of de detectie van door wachtwoord beveiligde archieven uitschakelen.
3. In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde malware of isoleert het programma geïnfecteerde bestanden in quarantaine.Als er na de scan niet opgeloste bedreigingen zijn, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

   Opmerking
   Houd ermee rekening dat er geen actie kan worden ondernomen op geïnfecteerde of verdachte bestanden die op cd's/dvd's zijn gevonden. Zo kan er ook geen actie worden ondernemen op geïnfecteerde of verdachte bestanden die zijn gedetecteerd op toegewezen netwerkstations als u niet over de geschikte privileges beschikt.

4. Nadat de scan is voltooid, wordt het venster met de scanresultaten weergegeven om u te laten weten of u de bestanden op de verwisselbare media veilig kunt openen.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een door malware geïnfecteerde cd/dvd gebruikt. De malware kan niet van de schijf worden verwijderd (het medium is alleen-lezen).Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat malware zich over uw systeem verspreidt.De beste werkwijze is het kopiëren van alle waardevolle gegevens van de schijf naar uw systeem en ze daarna verwijderen van de schijf.
- In sommige gevallen zal Bitdefender niet in staat zijn malware te verwijderen uit specifieke bestanden vanwege wettelijke of technische beperkingen. Een voorbeeld hiervan zijn bestanden die gearchiveerd zijn met een eigen technologie (dit is te wijten aan het feit dat het archief niet correct opnieuw kan worden gemaakt).

  Raadpleeg "*Malware van uw systeem verwijderen*" (p. 131) voor meer informatie over het omgaan met malware.

5.3.2. Scan verwisselbare media beheren

Volg deze stappen om het automatisch scannen van verwisselbare media te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Kies in het gedeelte **Scan gedetecteerde apparaten** de types opslagapparaten die u automatisch wilt laten scannen.Klik op de schakelaars om het automatisch scannen in of uit te schakelen.

Voor de beste beveiliging is het aanbevolen het automatisch scannen in te schakelen voor alle types verwisselbare opslagapparaten.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten.Als er geïnfecteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de malwarecode verwijderen) of ze naar quarantaine te verplaatsen. Als beide acties mislukken, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden.De scanopties zijn standaard en u kunt ze niet wijzigen.

5.4. Scanuitsluitingen configureren

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen. Deze functie is bedoeld om te vermijden dat u in uw werk wordt gestoord en kan ook helpen de systeemprestaties te verbeteren.Uitsluitingen zijn voorzien voor gebruikers die over een gevorderde computerkennis beschikken. Als u deze kennis niet hebt, kunt u de aanbevelingen van een expert van Bitdefender volgen.

U kunt uitsluitingen configureren die u wilt toepassen op Scannen bij toegang of Scannen op aanvraag afzonderlijk, of op beide scantypes tegelijk.De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.

Opmerking

Uitsluitingen komen NIET in aanmerking voor contextueel scannen.Contextueel scannen is een type van scannen op aanvraag. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met Bitdefender**.

5.4.1. Bestanden of mappen uitsluiten van het scannen

Volg deze stappen om specifieke bestanden of mappen uit te sluiten van het scannen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Schakel scanuitsluitingen voor bestanden in met de overeenkomende schakelaar.
5. Klik op de koppeling **Uitgesloten bestanden en mappen**.In het venster dat verschijnt, kunt u de bestanden en mappen die van het scannen zijn uitgesloten, beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
   b. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**.Daarnaast kunt u ook het pad naar het bestand of de map in het bewerkingsveld typen (of kopiëren en plakken).
   c. Het geselecteerde bestand of de geselecteerde map wordt standaard uitgesloten van Scannen bij toegang en Scannen bij aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.
   d. Klik op **Toevoegen**.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

5.4.2. Bestandsextensies uitsluiten van het scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender niet langer bestanden met die extensie scannen, ongeacht hun locatie op uw computer.De uitsluiting is ook van toepassing op bestanden op verwisselbare media, zoals cd's, dvd's, USB-opslagapparaten of netwerkstations.

Belangrijk
Ga voorzichtig te werk wanneer u extensies uitsluit van het scannen, want dergelijke uitsluitingen kunnen uw computer kwetsbaar maken voor malware.

Volg deze stappen om bestandsextensies uit te sluiten van het scannen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Schakel scanuitsluitingen voor bestanden in met de overeenkomende schakelaar.
5. Klik op de koppeling **Uitgesloten extensies**.In het venster dat verschijnt, kunt u de bestandsextensies die van het scannen zijn uitgesloten, beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
   b. Voer de extensies in die u wilt uitsluiten van het scannen en scheid ze van elkaar met puntkomma's (;).Hier is een voorbeeld:

      ```
      txt;avi;jpg
      ```

   c. Alle bestanden met de opgegeven extensies worden standaard uitgesloten van Scannen bij toegang en Scannen op aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.
   d. Klik op **Toevoegen**.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

5.4.3. Scanuitsluitingen beheren

Als de geconfigureerde scanuitsluitingen niet langer nodig zijn, is het aanbevolen dat u ze verwijdert of dat u scanuitsluitingen uitschakelt.

Volg deze stappen om de scanuitsluitingen te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.Gebruik de opties in het gedeelte **Bestanden en mappen** om scanuitsluitingen te beheren.
4. Klik op een van de beschikbare koppelingen om scanuitsluitingen te verwijderen of te bewerken.Ga als volgt te werk:
   - Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

- Om een gegeven in de tabel te bewerken, dubbelklikt u op dit item (of selecteert u het en klikt u op de knop **Bewerken**).Er verschijnt een nieuw venster. Hier kunt u de extensie of het pad dat moet worden uitgesloten en het type scan waarvoor u ze wilt uitsluiten, wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.

5. Gebruik de overeenkomende schakelaar voor het uitschakelen van scanuitsluitingen.

5.5. Bestanden in quarantaine beheren

Bitdefender isoleert de door malware geïnfecteerde bestanden die het niet kan desinfecteren en de verdachte bestanden in een beveiligd gebied dat de quarantaine wordt genoemd.Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender.Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

Daarnaast scant Bitdefender de bestanden in quarantaine na elke update van malware-handtekening.Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

Volg deze stappen om de bestanden in quarantaine te controleren en te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Quarantaine**.
4. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen.Hoewel dit niet aanbevolen is, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur.

   Quarantaine opnieuw scannen na updaten van virusdefinities

   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de virusdefinities.Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

   Verzend de bestanden in quarantaine naar Bitdefender voor verdere analyse

   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch naar Bitdefender te verzenden.De voorbeeldbestanden worden geanalyseerd door de malwareonderzoekers van Bitdefender.Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

Inhoud ouder dan {30} dagen verwijderen
Standaard worden bestanden in quarantaine die ouder zijn dan 30 dagen, automatisch verwijderd.Als u dit interval wilt wijzigen, geeft u een nieuwe waarde op in het overeenkomende veld.Typ 0 om het automatisch verwijderen van oude bestanden in quarantaine uit te schakelen.

5. Om een bestand in quarantaine te verwijderen, selecteert u het en klikt u op de knop **Verwijderen**.Als u een bestand uit quarantaine wilt terugzetten op zijn oorspronkelijke locatie, selecteert u het en klikt u op **Herstellen**.

5.6. Actief virusbeheer

Bitdefender Actief virusbeheer is een innovatieve proactieve detectietechnologie die geavanceerde heuristische methoden gebruikt voor het in real time detecteren van nieuwe potentiële bedreigingen.

Actief virusbeheer bewaakt voortdurende de toepassingen die op de computer worden uitgevoerd en zoekt naar acties die op malware lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend.Wanneer de algemene score voor een proces een bepaalde drempel bereikt, wordt het proces beschouwd als schadelijk en wordt het automatisch geblokkeerd.

Als Auto Pilot uit is, wordt u op de hoogte gebracht via een pop-upvenster over de geblokkeerde toepassing.Anders wordt de toepassing geblokkeerd zonder enige melding.U kunt controleren welke toepassingen zijn gedetecteerd door Actief virusbeheer in het venster Gebeurtenissen.

5.6.1. Gedetecteerde toepassingen controleren

Volg deze stappen om de toepassingen die zijn gedetecteerd door Actief virusbeheer, te controleren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Actief virusbeheer**.
4. Klik op een gebeurtenis om details erover weer te geven.
5. Als u de toepassing vertrouwt, kunt u Actief virusbeheer configureren om deze niet meer te blokkeren door op **Toestaan en bewaken** te klikken.Actief virusbeheer blijft doorgaan om de uitgesloten toepassingen te bewaken. Als voor een uitgesloten toepassing wordt vastgesteld dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis gewoon aangemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

5.6.2. Actief virusbeheer in- of uitschakelen

Volg deze stappen om Actief virusbeheer in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Klik op de schakelaars om deze optie in of uit te schakelen.

5.6.3. De bescherming van Antivirusbeheer aanpassen

Als u merkt dat Actief virusbeheer vaak rechtmatige toepassingen detecteert, moet u een toegeeflijker beveiligingsniveau instellen.

Volg deze stappen om de bescherming door Actief virusbeheer aan te passen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Controleer of Actief virusbeheer is ingeschakeld.
5. Sleep de schuifregelaar langs de schaal om het gewenste beveiligingsniveau in te stellen.Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

Opmerking

Wanneer u het beveiligingsniveau hoger instelt, zal Actief virusbeheer minder tekenen van malware-achtig gedrag vereisen om een proces te rapporteren. Dit zal leiden tot een hoger aantal gerapporteerde toepassingen en tegelijk, tot een grotere waarschijnlijkheid van valse positieven (veilige toepassingen die worden gedetecteerd als boosaardig).

5.6.4. Uitgesloten processen beheren

U kunt de uitsluitingsregels configureren voor vertrouwde toepassingen zodat Actief virusbeheer ze niet blokkeert als ze acties uitvoeren die op malware lijken.Actief virusbeheer blijft doorgaan om de uitgesloten toepassingen te bewaken. Als voor een uitgesloten toepassing wordt vastgesteld dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis gewoon aangemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

Volg deze stappen om de uitsluitingen voor het proces van Actief virusbeheer te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Klik op de koppeling **Uitgesloten processen**.In het venster dat verschijnt, kunt u de uitsluitingen voor het proces Actief virusbeheer beheren.

   Opmerking
   Procesuitsluitingen zijn ook van toepassing op het inbraakdetectiesysteem dat in de Bitdefender-firewall is inbegrepen.

5. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
   b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.
   c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief virusbeheer de toepassing blokkeert.
   d. Klik op **Toevoegen**.
6. Ga als volgt te werk om uitsluitingen te verwijderen of te bewerken:
   - Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.
   - Om een gegeven in de tabel te bewerken, dubbelklikt u op dit item (of selecteert u het en klikt u op de knop **Bewerken**).Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

5.7. Systeemkwetsbaarheden oplossen

Een belangrijke stap bij het beschermen van uw computer tegen kwaadwillende personen en applicaties is het up-to-date houden van het besturingssysteem en van de applicaties die u regelmatig gebruikt.Wij raden u ook aan te overwegen om de Windows-instellingen die het systeem kwetsbaarder maken voor malware, uit te schakelen.Bovendien moeten, om onbevoegden de toegang tot uw computer te ontzeggen, sterke wachtwoorden (wachtwoorden die moeilijk te raden zijn) voor elke Windows gebruikersaccount zijn geconfigureerd.

Bitdefender biedt twee eenvoudige manieren om de kwetsbaarheden van uw systeem op te lossen:

- U kunt uw systeem scannen op kwetsbaarheden en ze stapsgewijs repareren met de wizard **Kwetsbaarheidscan**.

- Met de automatische kwetsbaarheidsbewaking kunt u de gedetecteerde kwetsbaarheden controleren en oplossen in het venster Gebeurtenissen.

Het is aanbevolen de systeemkwetsbaarheden om de week of twee weken te controleren en op te lossen.

5.7.1. Uw systeem scannen op kwetsbaarheden

Volg deze stappen om systeemkwetsbaarheden op te lossen met de wizard Kwetsbaarheidscan:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antivirus**.
3. Klik op **Nu scannen** en selecteer vervolgens **Kwetsbaarheidscan**.
4. Volg de begeleide procedure van zes stappen om kwetsbaarheden van uw systeem te verwijderen.Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

   a. **Uw pc beveiligen**

   Selecteer de kwetsbaarheden die u wilt controleren.

   b. **Controleren op problemen**

   Wacht tot Bitdefender om de controle van uw systeem op kwetsbaarheden, te voltooien.

   c. **Windows updates**

   U ziet de lijst van kritieke en niet-kritieke Windows updates die niet zijn geïnstalleerd op uw computer.Selecteer de updates die u wilt installeren.

   Klik op **Volgende** om de installatie van de geselecteerde updates te starten.De installatie van de updates kan even duren en voor sommige updates zal het nodig zijn het systeem opnieuw op te starten om de installatie te voltooien.Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

   d. **Toepassingsupdates**

   Als een applicatie niet up-to-date is, klik dan op de getoonde link om de laatste versie te downloaden.

   e. **Zwakke wachtwoorden**

   U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw computer en de beschermingsniveaus van de wachtwoorden.

   Klik op **Herstellen** om de zwakke wachtwoorden te wijzigen.U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen.Voor een sterk wachtwoord

gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

f. **Summary**

Hier kunt u het resultaat van de bewerking bekijken.

5.7.2. De automatische kwetsbaarheidsbewaking gebruiken

Bitdefender scant uw systeem regelmatig op de achtergrond op kwetsbaarheden en houdt gegevens bij van de gevonden problemen in het venster Gebeurtenissen.

Volg deze stappen om de gedetecteerde problemen te controleren en op te lossen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Kwetsbaarheid**.
4. U kunt gedetailleerde informatie betreffende de gedetecteerde kwetsbaarheden van het systeem zien.Afhankelijk van het probleem, gaat u als volgt te werk om een specifieke kwetsbaarheid te herstellen:
   - Als er Windows-updates beschikbaar zijn, klikt u op **Nu bijwerken** om de wizard Kwetsbaarheidscan te openen en de updates te installeren.
   - Als een toepassing verouderd is, klikt u op **Nu bijwerken** om een koppeling te zoeken naar de webpagina van de verkoper vanaf waar u de nieuwste versie van die toepassing kunt installeren.
   - Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **Wachtwoord herstellen** om de gebruiker te forceren het wachtwoord te wijzigen bij de volgende aanmelding of wijzigt u zelf het wachtwoord.Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).
   - Als de Windows-functie Autorun is ingeschakeld, klikt u op **Uitschakelen** om de functie uit te schakelen.

Volg deze stappen om de instellingen voor de kwetsbaarheidsbewaking te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Kwetsbaarheid**.
4. Klik op de schakelaar om Automatische kwetsbaarheidscan in of uit te schakelen.

Belangrijk

Om automatisch op de hoogte te worden gebracht over kwetsbaarheden van het systeem of de toepassing, moet u **Automatische kwetsbaarheidscan** ingeschakeld houden.

5. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.

Kritieke Windows updates

Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.

Normale Microsoft updates

Controleer of uw Windows-besturingssysteem over de laatste gewone beveiligingsupdates van Microsoft beschikt.

Toepassingsupdates

Controleer of cruciale webverwante toepassingen die op uw systeem zijn geïnstalleerd, up-tot-date zijn.Verouderde toepassingen kunnen door kwaadaardige software worden misbruikt, waardoor uw pc kwetsbaar wordt voor aanvallen van buitenaf.

Zwakke wachtwoorden

Controleer of de wachtwoorden van de Windows-accounts die op het systeem zijn geconfigureerd, gemakkelijk te raden zijn.Het instellen van moeilijk te raden wachtwoorden (sterke wachtwoorden) maakt het bijzonder moeilijk voor hackers om in uw systeem in te breken.Een sterk wachtwoord bevat hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $ of @).

Autorun media

Controleer de status van de Windows-functie Autorun.Met deze functie kunnen toepassingen automatisch worden gestart vanaf cd's, dvd,'s, USB-stations of andere externe apparaten.

Sommige malwaretypes gebruiken Autorun om zich automatisch te verspreiden vanaf de verwisselbare media naar de pc. Daarom is het aanbevolen deze Windows-functie uit te schakelen.

Opmerking

Als u de bewaking van een specifieke kwetsbaarheid uitschakelt, worden verwante problemen niet langer opgenomen in het venster Gebeurtenissen.

6. Antispam

Spam is een term die wordt gebruikt voor het beschrijven van ongewenste e-mail.Spam betekent zowel voor individuele gebruikers als voor bedrijven een steeds groter probleem. Het is niet mooi, u wilt niet dat uw kinderen het zien, u kunt erdoor ontslagen worden (omdat u teveel tijd verspilt of omdat u porno ontvangt in uw zakelijke e-mail) en u kunt niet verhinderen dat men u deze berichten blijft zenden. De op één na beste oplossing ligt dus voor de hand: de ontvangst van dergelijke berichten blokkeren. Jammer genoeg komen spamberichten voor in allerlei vormen en formaten en op zeer grote schaal.

Bitdefender Antispam gebruikt opmerkelijke technologische innovaties en industriestandaard antispamfilters om spam op te sporen voordat deze het Postvak IN van de gebruiker bereikt.Meer informatie vindt u onder *"Antispam-begrippen"* (p. 65).

De antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol.POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver.

Opmerking

Bitdefender biedt geen antispambeveiliging voor e-mailaccounts die u aanspreekt via een e-mailservice op internet.

De spamberichten die door Bitdefender worden gedetecteerd, zijn gemarkeerd met de prefix [spam] in de onderwerpregel.Bitdefender verplaatst spamberichten automatisch naar een specifieke map, zoals hieronder beschreven:

- In Microsoft Outlook worden spamberichten verplaatst naar een map **Spam** die zich in de map **Verwijderde items** bevindt.De map **Spam** wordt gemaakt tijdens de installatie van Bitdefender.
- In Outlook Express en Windows Mail worden spamberichten direct naar **Verwijderde items** verplaatst.
- In Mozilla Thunderbird worden spamberichten verplaatst naar een map **Spam** die zich in de map **Trash** bevindt.De map **Spam** wordt gemaakt tijdens de installatie van Bitdefender.

Als u andere e-mailclients gebruikt, moet u een regel maken voor het verplaatsen van de e-mailberichten die zijn gemarkeerd als [spam] via Bitdefender naar een aangepaste quarantainemap.

6.1. Antispam-begrippen

6.1.1. Antispam-filters

De Bitdefender Antispam-engine bevat meerdere filters die garanderen dat uw Postvak IN vrij blijft van SPAM: Vriendenlijst, Spammerslijst, Tekensetfilter, Verbindingsfilter, Handtekeningenfilter, NeuNet-filter (heuristisch) en in-the-cloud-detectie.

Vriendenlijst / Spammerslijst

De meeste mensen communiceren regelmatig met een groep mensen of ontvangen zelfs berichten van bedrijven of organisaties in hetzelfde domein. Wanneer u gebruik maakt van **vrienden- of spammerslijsten**, kan u gemakkelijk een indeling maken van de mensen van wie u e-mails wilt ontvangen, ongeacht de inhoud (vrienden), of van de mensen van wie u nooit meer wilt horen (spammers).

Opmerking

Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. Bitdefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

Tekensetfilter

Heel wat spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. Het tekensetfilter detecteert dit type berichten en labelt ze als SPAM.

Link filter

Bijna alle spamberichten bevatten koppelingen naar verschillende weblocaties. Deze locaties bevatten doorgaans meer reclame en de mogelijkheid om zaken te kopen. Bovendien worden ze soms ook gebruikt voor phishing.

Bitdefender houdt een database bij van dergelijke koppelingen.De Koppelingsfilter controleert elke URL-koppeling in een bericht ten opzichte van zijn database. Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

Handtekeningenfilter

De spamonderzoekers van Bitdefender analyseren voortdurend de spam-e-mails in het wild en geven spamhandtekeningen vrij waarmee deze e-mails kunnen worden gedetecteerd.

De Handtekeningenfilter controleert e-mails ten opzichte van de spamhandtekeningen in de lokale database.Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

Opmerking
In tegenstelling tot de andere filters, kan de Handtekeningenfilter niet onafhankelijk van de antispambescherming worden uitgeschakeld.

NeuNet (Heuristische) filter

De **NeuNet (Heuristische) filter** voert een aantal tests uit op alle componenten van het bericht (dus niet alleen op de koptekst, maar ook op het hoofdbericht in HTML- of tekstindeling). Hierbij wordt gezocht naar woorden, zinnen, koppelingen of andere kenmerken van SPAM.Op basis van de resultaten van de analyse, zal de e-mail een spamscore ontvangen.

Als de spamscore het drempelniveau overschrijdt, wordt de e-mail beschouwd als SPAM.Het drempelniveau wordt bepaald door het antispamgevoeligheidsniveau.Meer informatie vindt u onder “*Het gevoeligheidsniveau aanpassen*” (p. 72).

De filter detecteert ook berichten die in de onderwerpregel zijn gemarkeerd als `SEXUALLY-EXPLICIT:` en labelt ze als SPAM.

Opmerking
Sinds 19 mei 2004 moet spam met seksueel gericht materiaal de waarschuwing `SEXUALLY-EXPLICIT:` bevatten in de onderwerpregel anders kunnen boeten worden opgelegd voor het overtreden van de nationale wetgeving.

In-the-cloud detectie

“In-the cloud”-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

E-mails worden alleen “in the cloud” gecontroleerd als de lokale antispamfilters geen afdoend resultaat bieden.

6.1.2. Antispamgebruik

De Bitdefender Antispam-engine gebruikt alle antispamfilters samen om vast te stellen of een bepaald e-mailbericht in uw **Postvak IN** moet belanden.

Elke e-mail die van het internet komt, wordt eerst gecontroleerd met Vriendenlijst/Spammerslijst filter. Als het adres van de afzender in de Vriendenlijst wordt gevonden, wordt de e-mail rechtstreeks naar uw **Postvak IN** verplaatst.

In het andere geval zal de filter Spammerslijst de e-mail overnemen om het adres van de afzender te controleren in zijn lijst. Als er een treffer wordt gevonden, wordt de e-mail gelabeld als SPAM en naar de map **Spam** verplaatst.

Anders zal de Tekensetfilter controleren of de e-mail in Cyrillische of Aziatische tekens is geschreven. Als dat het geval is, wordt de e-mail gelabeld als SPAM en verplaatst naar de map **Spam**.

De Verbindingsfilter zal de koppelingen die in de e-mail zijn gevonden, vergelijken met de koppelingen van de Bitdefender-database van bekende spamkoppelingen. In geval van overeenkomst, wordt de e-mail als SPAM beschouwd.

Vervolgens controleert de Handtekeningenfilter de e-mail ten opzichte van de spamhandtekeningen in de lokale database.Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

De NeuNet-filter (heuristisch) zal de e-mail overnemen en een aantal tests uitvoeren op alle componenten van het bericht, waarbij wordt gezocht naar woorden, zinnen, koppelingen of andere kenmerken van spam.Op basis van de resultaten van de analyse, zal de e-mail een spamscore ontvangen.

Opmerking

Als de e-mail het label SEXUALLY EXPLICIT vermeldt in de onderwerpregel, zal Bitdefender dit bericht als SPAM beschouwen.

Als de spamscore het drempelniveau overschrijdt, wordt de e-mail beschouwd als SPAM.Het drempelniveau wordt bepaald door het antispambeveiligingsniveau.Meer informatie vindt u onder *"Het gevoeligheidsniveau aanpassen"* (p. 72).

Als de lokale antispamfilters geen afdoend resultaat bieden, wordt de e-mail gecontroleerd met "in-the-cloud" detectie die uiteindelijk beslist of de e-mail spam of rechtmatig is.

6.1.3. Antispam-updates

Telkens wanneer een update wordt uitgevoerd, worden nieuwe handtekeningen voor bekende spam-e-mails en koppelingen toegevoegd aan de databases.Dit zal de doeltreffendheid van uw Antispam-engine verbeteren.

Bitdefender kan automatische updates uitvoeren om u te beschermen tegen spammers. Houd de optie **Automatische update** ingeschakeld.

6.1.4. Ondersteunde e-mailclients en protocollen

Antispam bescherming is aanwezig voor alle POP3/SMTP e-mailclients.De Bitdefender Antispam werkbalk is echter alleen geïntegreerd in:

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express en Windows Mail (op 32-bits systemen)
- Mozilla Thunderbird 3.0.4

6.2. De antispambeveiliging in- of uitschakelen

Volg deze stappen om de antispambeveiliging in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antispam**.

3. Klik op de schakelaar om de antispambeveiliging in of uit te schakelen.

6.3. De antispam-werkbalk in het venster van uw e-mailclient gebruiken

In het bovenste gebied van het venster van de e-mailclient ziet u de werkbalk Antispam.De werkbalk Antispam helpt u de antispambeveiliging direct vanaf uw e-mailclient te beheren.U kunt Bitdefender gemakkelijk corrigeren als het programma een rechtmatig bericht als SPAM heeft gemarkeerd.

Belangrijk

Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk.Raadpleeg "*Ondersteunde e-mailclients en protocollen*" (p. 67) voor een complete lijst van ondersteunde e-mailclients.

Elke knop van de Bitdefender-werkbalk wordt hieronder uitgelegd.

Is spam - geeft aan dat de geselecteerde e-mail spam is.De e-mail wordt onmiddellijk naar de map **Spam** verplaatst.Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.

Geen spam - geeft aan dat de geselecteerde e-mail geen spam is en dat Bitdefender het niet als dusdanig mocht labelen.De e-mail wordt van de map **Spam** verplaatst naar de map van uw **Postvak IN**.Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.

Belangrijk

De knop **Geen spam** wordt actief wanneer u een bericht selecteert dat door Bitdefender als SPAM is gemarkeerd (normaal bevinden deze berichten zich in de map **Spam**).

Spammer toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de spammerslijst.U zult mogelijk op **OK** moeten klikken om te bevestigen.De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als `[spam]`.

Vriend toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de vriendenlijst.U zult mogelijk op **OK** moeten klikken om te bevestigen.U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

Spammers - opent de **Spammerslijst** die alle e-mailadressen bevatten waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud.Meer informatie vindt u onder "*Spammerslijst configureren*" (p. 71).

Vrienden - opent de **Vriendenlijst** die alle e-mailadressen bevatten waarvan u altijd e-mailberichten wilt ontvangen, ongeacht hun inhoud.Meer informatie vindt u onder “*De Vriendenlijst configureren*” (p. 70).

Instellingen - opent een venster waarin u de antispamfilters en de werkbalkinstellingen kunt configureren.

6.3.1. Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet zijn gemarkeerd als [spam]). Hierdoor helpt u de efficiëntie van de antispamfilter verbeteren.Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als [spam].
4. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender om de afzender aan de vriendenlijst toe te voegen.U zult mogelijk op **OK** moeten klikken om te bevestigen.U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
5. Klik op de knop **Geen spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient).Het e-mailbericht wordt verplaatst naar de map Postvak IN.

6.3.2. Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor helpt u de efficiëntie van de antispamfilter verbeteren.Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

6.3.3. Werkbalkinstellingen configureren

Om de instellingen voor antispam-werkbalk te configureren, klikt u op de knop **Instellingen** op de werkbalk en vervolgens op het tabblad **Instellingen werkbalk** .

De instellingen zijn gegroepeerd in twee categorieën:

- In de categorie **E-mailregels** kunt u de verwerkingsregels configureren voor de spam-e-mails die door Bitdefender zijn gedetecteerd.
  - **Bericht verplaatsen naar Verwijderde items** (alleen voor Microsoft Outlook Express / Windows Mail)

    Opmerking
    In Microsoft Outlook /Mozilla Thunderbird worden gedetecteerde spamberichten automatisch verplaatst naar een Spam-map die zich in de map Verwijderde items / Trash bevindt.

  - **Markeer e-mailberichten met spam als 'gelezen'** - markeert spamberichten automatisch als gelezen, zodat u er niet door wordt gestoord als ze aankomen.
- In de categorie **Meldingen** kunt u kiezen of u bevestigingsvensters wilt weergeven wanneer u in de antispam-werkbalk op de knoppen **Spammer toevoegen** en **Vriend toevoegen** klikt.Bevestigingsvensters kunnen verhinderen dat u e-mailafzenders per ongeluk toevoegt aan een Vrienden-/Spammerslijst.

6.4. De Vriendenlijst configureren

De **Vriendenlijst** is een lijst van alle e-mailadressen waarvan u altijd berichten wilt ontvangen, ongeacht hun inhoud. Berichten van uw vrienden zijn niet als spam gelabeld, zelfs wanneer de inhoud op spam lijkt.

Opmerking
Elke e-mail die afkomstig is van een adres in de **Vriendenlijst**, wordt automatisch en zonder verdere verwerking in uw Postvak IN geleverd.

De Vriendenlijst configureren en beheren:

- Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, klikt u op de knop **Vrienden** in de antispam-werkbalk van Bitdefender die in uw e-mailclient is geïntegreerd.
- U kunt ook deze stappen volgen:
  1. Open het Bitdefender-venster.
  2. Ga naar het deelvenster **Antispam**.
  3. Klik op **Beheren** en kies **Vrienden** in het menu.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**.Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**.Syntaxis:

- @domein.com, *domein.com en domein.com - alle ontvangen e-mailberichten van domein.com zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *com* - alle ontvangen e-mailberichten die het domeinachtervoegsel com hebben, zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn.U kunt bijvoorbeeld het e-maildomein toevoegen van het bedrijf waarvoor u werkt of de domeinen van uw vertrouwde partners toevoegen.

Om een item uit de lijst te verwijderen, klikt u op de overeenkomende koppeling **Verwijderen**.Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product.Om de vriendenlijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie.Het bestand zal de extensie `.bwl` hebben.

Om een eerder opgeslagen vriendenlijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende `bwl`-bestand.Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

6.5. Spammerslijst configureren

De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud.Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.

De Spammerslijst configureren en beheren:

- Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, klikt u op de knop **Spammers** in de antispamwerkbalk van Bitdefender die in uw e-mailclient is geïntegreerd.
- U kunt ook deze stappen volgen:
  1. Open het Bitdefender-venster.
  2. Ga naar het deelvenster **Antispam**.
  3. Klik op **Beheren** en kies **Spammers** in het menu.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**.Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**.Syntaxis:

- @domain.com, *domain.com and domain.com - alle ontvangen e-mailberichten van domein.com worden als SPAM gelabeld;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) worden als SPAM gelabeld;
- *com* - alle ontvangen e-mailberichten met het domeinachtervoegsel com worden als SPAM gelabeld.

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn.

Waarschuwing

Voeg geen domein van rechtmatige e-mailservices via het web (zoals Yahoo, Gmail, Hotmail of andere) toe aan de Spammerslijst. Anders zullen de e-mailberichten die zijn ontvangen van een geregistreerde gebruiker van een dergelijke service, als spam worden gedetecteerd.Als u bijvoorbeeld `yahoo.com` toevoegt aan de spammerslijst, worden alle e-mailberichten die van adressen van `yahoo.com` afkomstig zijn, als `[spam]` gemarkeerd.

Om een item uit de lijst te verwijderen, klikt u op de overeenkomende koppeling **Verwijderen**.Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de spammerslijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product.Om de spammerslijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie.Het bestand zal de extensie `.bwl` hebben.

Om een eerder opgeslagen Spammerslijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bwl-bestand.Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

6.6. Het gevoeligheidsniveau aanpassen

Als u merkt dat sommige rechtmatige e-mails als spam zijn gemarkeerd of dat heel wat spam-e-mails niet gedetecteerd worden, kunt u proberen het niveau voor de antispamgevoeligheid aan te passen om het probleem op te lossen.In plaats van het gevoeligheidsniveau onafhankelijk te wijzigen, is het echter aanbevolen dat u eerst “*De antispamfilter werkt niet goed*” (p. 124) leest en de instructies volgt om het probleem te corrigeren.

Volg deze stappen om het antispamgevoeligheidsniveau aan te passen:

1. Bitdefender openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antispam** en klik vervolgens op het tabblad **Instellingen**.
4. Gebruik de beschrijving aan de rechterzijde van de schaal om het gevoeligheidsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.De beschrijving informeert u ook over alle extra acties die u moet ondernemen om potentiële problemen te vermijden of de efficiëntie van de antispamdetectie te verhogen.

6.7. De lokale antispamfilters configureren

Zoals beschreven in "*Antispam-begrippen*" (p. 65), gebruikt Bitdefender een combinatie van verschillende antispamfilters voor het identificeren van spam.De antispamfilters zijn vooraf geconfigureerde voor een efficiënte bescherming.

Belangrijk

Afhankelijk van het feit of rechtmatige e-mails ontvangt in Aziatische of Cyrillische tekens, kunt u de instelling die dergelijke e-mails blokkeert, in- of uitschakelen.De overeenkomende instelling is uitgeschakeld in de gelokaliseerde versies van het programma die dergelijke tekensets gebruiken (bijvoorbeeld in de Russische of Chinese versie).

Volg deze stappen om de lokale antispamfilters te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antispam** en klik vervolgens op het tabblad **Instellingen**.
4. Klik op de schakelaars om de lokale antispamfilters in of uit te schakelen.

Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, kunt u de lokale antispamfilters direct vanaf uw e-mailclient configureren.Klik op de knop **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient) en klik vervolgens op het tabblad **Antispamfilters**.

6.8. In-the-cloud detectie configureren

"In-the cloud"-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

Volg deze stappen om een "in the cloud"-detectie te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antispam** en klik vervolgens op het tabblad **Cloud**.
4. Klik op de schakelaar om de “in-the-cloud”-detectie in of uit te schakelen.
5. Voorbeelden van rechtmatige e-mails of spam-e-mails kunnen worden verzonden naar Bitdefender Cloud wanneer u detectiefouten of niet-gedetecteerde spam-e-mails aanduidt. Hiermee kan de antispam-detectie van Bitdefender worden verbeterd.Configureer het verzenden van e-mailvoorbeelden naar Bitdefender Cloud door de gewenste opties te selecteren.

Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, kunt u “in-the-cloud”-detectie direct vanaf uw e-mailclient configureren.Klik op de knop **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient) en klik vervolgens op het tabblad **Cloud-instellingen**.

7. Privacybeheer

Uw persoonlijke informatie is een constant doelwit voor cybercriminelen.Als de bedreigingen zich hebben uitgebreid tot nagenoeg het volledige spectrum van uw online activiteiten, kan onvoldoende beschermde e-mail, Instant messaging en surfen op het web leiden tot informatielekken die uw privacy in gevaar brengen.

Bitdefender Privacybeheer gaat al deze bedreigingen te lijf met meerdere componenten.

- Antiphishing-beveiliging - biedt een uitgebreide reeks functies waarmee uw systeem wordt beschermd terwijl u surft op internet. Deze optie verhindert dat u persoonlijke informatie bekendmaakt aan frauduleuze websites die zich voordoen als rechtmatig.
- Gegevensbeveiliging - helpt u ervoor te zorgen dat uw persoonlijke informatie niet vanaf uw computer wordt verzonden zonder uw toestemming.Deze optie scant e-mails en expresberichten die vanaf uw computer zijn verzonden en gegevens die via webpagina's zijn verzonden en blokkeert alle informatie die wordt beschermd door de regels voor Gegevensbeveiliging die u hebt gemaakt.
- Chat encryptie - codeert uw IM-conversaties zodat u zeker bent dat de inhoud vertrouwelijk blijft tussen u en uw chatpartner.

7.1. Antiphishing-beveiliging

Bitdefender Antiphishing dat persoonlijke informatie over u wordt onthuld, als u over het Internet surft, door u te waarschuwen voor potentiële phishing webpagina's.

Bitdefender biedt real-time antiphishing beschermingvoor:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Volg deze stappen om de Antiphishing-instellingen te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Privacybeheer** en klik vervolgens op het tabblad **Antiphishing**.

De instellingen zijn gegroepeerd in twee categorieën.

Functies werkbalk

Klik op de schakelaars om deze optie in of uit te schakelen.

- De Bitdefender-werkbalk in de webbrowser weergeven.
- Search advisor, een component die de resultaten van uw zoekacties op Google, Bing en Yahoo! en van de koppelingen van Facebook en Twitter beoordeelt door een pictogram voor elk resultaat te plaatsen:

  U mag deze webpagina niet bezoeken.

  Deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

  Dit is een pagina die u veilig kunt bezoeken.

- SSL-webverkeer scannen.

  Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden.Het is daarom aanbevolen SSL scannen in te schakelen.

Bescherming voor webbrowsers

Klik op de schakelaars om deze optie in of uit te schakelen.

- Bescherming tegen fraude.
- Bescherming tegen phishing.
- Bescherming voor instant messaging.

U kunt een lijst opmaken van websites die niet zullen worden gescand door de Antiphishing-engines van Bitdefender.De lijst mag websites bevatten die u volledig vertrouwt.Voeg bijvoorbeeld de websites toe waar u regelmatig online winkelt.

Klik op de koppeling **Witte lijst** om de witte lijst voor antiphishing te configureren en te beheren.Een nieuw venster wordt weergegeven.

Om een site toe te voegen aan de Witte lijst, geeft u het adres van de site op in het overeenkomende veld en kikt u op **Toevoegen**.

Om een website uit de lijst te verwijderen, selecteert u de site in de lijst en klikt u op de overeenkomende koppeling **Verwijderen**.

Klik op **Save** om de wijzigingen op te slaan en het venster te sluiten.

7.1.1. Bitdefender-bescherming in de webbrowser

Bitdefender wordt rechtstreeks in de volgende webbrowsers geïntegreerd door middel van een intuïtieve en gemakkelijk te gebruiken werkbalk:

- Internet Explorer
- Mozilla Firefox

- Google Chrome
- Safari
- Opera

De Bitdefender-werkbalk is niet uw standaard browserwerkbalk.Hiermee wordt alleen een kleine sleper bovenaan elke webpagina toegevoegd.Klik om de werkbalk weer te geven.

De werkbalk van Bitdefender bevat de volgende elementen:

Paginaclassificatie

Afhankelijk van de manier waarop Bitdefender de webpagina die u momenteel bekijkt classificeert, wordt een van de volgende classificaties weergegeven aan de linkerzijde van de werkbalk:

- Het bericht “Deze pagina is niet veilig” verschijnt op een rode achtergrond – u moet de webpagina onmiddellijk verlaten.
- Het bericht “Opgelet” verschijnt op een oranje achtergrond – deze webpagina kan gevaarlijke inhoud bevatten.Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.
- Het bericht “Deze pagina is veilig” verschijnt op een groen achtergrond – dit is een veilige pagina om te bezoeken.

Sandbox

Klik op om de browser te starten in een door Bitdefender geleverde omgeving, waarbij deze wordt geïsoleerd van het besturingssysteem.Hiermee wordt verhinderd dat op browsers gebaseerde bedreigingen kwetsbaarheden van de browser benutten om de controle over het systeem te krijgen.Gebruik Sandbox wanneer u webpagina’s bezoekt waarvan u vermoedt dat ze malware bevatten.

Opmerking
Sandbox is niet beschikbaar op computers met Windows XP.

Instellingen

Klik op om individuele functies in of uit te schakelen:

- Antiphishing Filter
- Antimalware-filter
- Search Advisor

Voedingsschakelaar

Om de werkbalkfuncties volledig in of uit te schakelen, klikt u rechts op de werkbalk op .

7.1.2. Bitdefender waarschuwt in de browser

Telkens wanneer u een website bezoekt die als onveilig is geclassificeerd, wordt de website geblokkeerd en wordt een waarschuwingspagina weergegeven in uw browser.

De pagina bevat informatie, zoals de URL van de website en de gedetecteerde bedreiging.

U moet beslissen wat u vervolgens wilt doen. De volgende opties zijn beschikbaar:

- Navigeer weg van de webpagina.
- U kunt ondanks de waarschuwing naar de webpagina gaan door op **Ik begrijp het risico, laat me er toch heengaan** te klikken.
- Voeg de pagina to aan de witte lijst voor Antiphishing door op **Toevoegen aan witte lijst** te klikken.De pagina wordt niet langer gescand door de antiphishing-engines van Bitdefender.

7.2. Data bescherming

De gegevensbescherming voorkomt dat vertrouwelijke gegevens lekken wanneer u online bent.

Stel u een eenvoudig voorbeeld voor: u hebt een regel voor de gegevensbeveiliging gemaakt die uw creditcardnummer beschermt.Als een spywareprogramma er echter op de een of andere manier in slaagt zich op uw computer te installeren, kan het uw creditcardnummer niet via e-mail, expresberichten of webpagina's verzenden.Bovendien kunnen uw kinderen het niet gebruiken om online te kopen of het bekendmaken aan mensen die ze op internet hebben ontmoet.

Raadpleeg de volgende onderwerpen voor meer informatie:

- “*Over gegevensbeveiliging*” (p. 78).
- “*Gegevensbeveiliging configureren*” (p. 79).
- “*Regels beheren*” (p. 80).

7.2.1. Over gegevensbeveiliging

Of het nu uw e-mail is of uw creditcardnummer, als deze gegevens in verkeerde handen terechtkomen, kunnen ze u schade berokkenen. U kan worden overspoeld door spamberichten of u kan plotseling voor een onaangename verrassing komen te staan als u ziet dat uw rekening is leeggeplunderd.

Op basis van de regels die u maakt, scant Gegevensbeveiliging het web, e-mail en IM-verkeer die uw computer verlaten op specifieke tekenreeksen (bijv. uw creditcardnummer). Als er een overeenkomst is, wordt de desbetreffende webpagina, de e-mail of het IM-bericht geblokkeerd.

U kan regels creëren voor het beveiligen van elke persoonlijke of vertrouwelijke informatie, van uw telefoonnummer of e-mailadres tot uw bankrekeninginformatie.Er is ondersteuning voorzien voor meerdere gebruikers, zodat andere gebruikers die zich aanmelden bij andere Windows-gebruikersaccounts hun eigen regels kunnen configureren en gebruiken.Als uw Windows-account een beheerdersaccount is, kunnen de regels die u maakt, worden geconfigureerd om deze ook toe te passen wanneer andere gebruikers van de computer zijn aangemeld op hun Windows-gebruikersaccounts.

7.2.2. Gegevensbeveiliging configureren

Volg deze stappen als u Identiteitscontrole wilt gebruiken:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Privacybeheer** en klik vervolgens op het tabblad **Gegevensbeveiliging**.
4. Zorg dat de gegevensbeveiliging is ingeschakeld.
5. Creëer regels om uw gevoelige data te beschermen.Meer informatie vindt u onder *"Regels voor de gegevensbeveiliging maken"* (p. 79).

Regels voor de gegevensbeveiliging maken

Om een regel te maken, klikt u op de knop **Regel toevoegen** en volgt u de configuratiewizard.Gebruik de knoppen **Volgende** en **Vorige** om te navigeren door de wizard.Klik op **Annuleren** om de wizard af te sluiten.

1. **Type en gegevens van de regel instellen**

   U moet de volgende parameters instellen:

   - **Regelnaam** - voer de naam van de regel in dit bewerkingsveld in.
   - **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, BSN, enz.).
   - **Regeldata** - voer de te beveiligen data in dit bewerkingsveld in.Bijvoorbeeld, als u uw credicardnummer wilt beveiligen, voer het dan hier in zijn geheel of gedeeltelijk in

     Belangrijk

     Als u minder dan drie tekens invoert, wordt u gevraagd de gegevens te valideren. Wij raden u aan minstens drie tekens in te voeren om te vermijden dat berichten en webpagina's ten onrechte worden geblokkeerd.

   Alle gegevens die u invoert, worden gecrypteerd. Voor extra veiligheid adviseren wij van de gegevens die u wilt beschermen niet alles in tevoeren.

2. **Verkeerstypes en gebruikers selecteren**

a. Selecteer het type verkeer dat u door Bitdefender wilt laten scannen.

- **Webverkeer (HTTP) scannen** - scant het HTTP-verkeer (web) en blokkeert de uitgaande gegevens die overeenkomen met de regelgegevens.
- **E-mail scannen (SMTP-verkeer)** - scant het SMTP-verkeer (e-mail) en blokkeert de uitgaande e-mailberichten die de regelgegevens bevatten.
- **IM-verkeer scannen (Instant Messaging)** - scant het IM-verkeer (expresberichten) en blokkeert de uitgaande chatberichten die de regelgegevens bevatten.

U kunt ervoor kiezen de regels alleen toe te passen als de regeldata overeenkomen met volledige woorden of als de regeldata en de gedetecteerde tekenreeks overeenkomen.

b. Geef de gebruikers op waarvoor de regel van toepassing is.

- **Alleen voor mij (huidige gebruiker)** - de regel zal alleen op uw gebruikersaccount van toepassing zijn.
- **Beperkte gebruikersaccounts** - de regel zal van toepassing zijn op u en alle beperkte Windows-accounts.
- **Alle gebruikers** - de regel zal van toepassing zijn op alle Windows-accounts.

3. **Regel beschrijven**

Voer een korte beschrijving in van de regel in het bewerkingsveld.Omdat de geblokkeerde data (tekenreeks) niet in normale tekst zichtbaar is als u de regel opent, kan u deze met de beschrijving beter herkennen.

Klik op **Voltooien**.De regels worden weergegeven in de tabel.

Vanaf nu zal elke poging tot het verzenden van de opgegeven gegevens (via e-mail, expresberichten of een webpagina) mislukken.Er verschijnt een item in het venster Gebeurtenissen dat aangeeft dat Bitdefender het verzenden van identiteitsspecifieke inhoud heeft geblokkeerd.

7.2.3. Regels beheren

De regels voor de gegevensbeveiliging beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Privacybeheer** en klik vervolgens op het tabblad **Gegevensbeveiliging**.

De regels die tot nu toe zijn gemaakt, worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Regel verwijderen**.

Om een regel te bewerken, selecteert u deze en klikt u op de knop **Regel bewerken**. Een nieuw venster wordt weergegeven.Hier kan u de naam, de beschrijving en de parameters (type, gegevens en verkeer) van de regel wijzigen. Klik op **OK** om de wijzigingen op te slaan.

7.3. Chat Encryptie

De inhoud van uw expresberichten zou alleen mogen bekend zijn voor u en uw chatpartner.Door uw conversaties te coderen, kunt u verhinderen dat iemand die ze probeert te onderscheppen naar en van uw contactpersonen, de inhoud kan lezen.

Standaard crypteert Bitdefender al uw instant messaging chatsessies, op voorwaarde dat:

- Uw chatpartner heeft een Bitdefender-product geïnstalleerd dat Chat Encryptie ondersteunt en Chat Encryptie is ingeschakeld voor de toepassing voor instant messaging die voor het chatten wordt gebruikt.
- U en uw chatpartner gebruiken ofwel Yahoo Messenger of Windows Live (MSN) Messenger.

Belangrijk

Bitdefender zal een conversatie niet coderen als een chatpartner een op het web gebaseerde chattoepassing gebruikt, zoals Meebo, of als een van de chatpartners Yahoo! gebruikt en de andere Windows Live (MSN).

De codering van expresberichten configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Privacybeheer** en klik vervolgens op het tabblad **Codering**.

Standaard is Chat Encryptie ingeschakeld voor zowel Yahoo Messenger en Windows Live (MSN) Messenger.U kunt Chat encryptie uitschakelen voor een of beide toepassingen door op de overeenkomende schakelaar te klikken.

8. Ouderlijk Toezicht

Met bitDefender Ouderlijk Toezicht kan u de toegang tot het Internet en tot specifieke toepassingen beheren voor elke gebruiker die een gebruikersaccount op het systeem heeft.

U kan Ouderlijk Toezicht configureren voor het blokkeren van:

- ongeschikte webpagina's.
- Toegang tot het Internet gedurende een bepaalde periode (bijvoorbeeld als het tijd is om huiswerk te maken).
- webpagina's, e-mailberichten en instant messages die bepaalde sleutelwoorden bevatten.
- applicaties zoals spelletjes, chatten, programma's die bestanden uitwisselen en dergelijke.
- instant messages van andere dan de toegelaten IM contacten.

Belangrijk

Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.Om er zeker van te zijn dat alleen u de instellingen van Ouderlijk Toezicht kan veranderen, kan u deze beveiligen met een wachtwoord

Zodra u Ouderlijk toezicht hebt geconfigureerd, kunt u gemakkelijk zien wat uw kinderen op de computer doen.

Zal wanneer u niet thuis bent, kunt u nog steeds de activiteiten van uw kinderen controleren en de instellingen voor Ouderlijk toezicht wijzigen via Ouderlijk toezicht op afstand.

8.1. Ouderlijk toezicht configureren

Voordat u Ouderlijk toezicht configureert, moet u afzonderlijke Windows-gebruikersaccounts maken voor uw kinderen. Hiermee weet u precies wat uw kinderen doen op de computer. U moet beperkte (standaard) gebruikersaccounts maken zodat ze de instellingen voor Ouderlijk toezicht niet kunnen wijzigen.Meer informatie vindt u onder “*Windows-gebruikersaccounts maken*” (p. 34).

Als uw kinderen toegang hebben tot een beheerdersaccount op hun computer, moet u een wachtwoord configureren om de instellingen voor Ouderlijk toezicht te beveiligen.Meer informatie vindt u onder “*Wachtwoordbeveiligde Bitdefender-instellingen*” (p. 18).

Ouderlijk toezicht configureren:

1. Zorg dat u bij de computer bent aangemeld met een beheerdersaccount.Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.
2. Open het Bitdefender-venster.
3. Klik op de knop **Instellingen** in de werkbalk bovenaan.
4. Klik in het menu aan de linkerzijde op **Ouderlijk toezicht** en klik vervolgens op het tabblad **Accounts**.Hier kunt u de instellingen voor Ouderlijk toezicht van elke Windows-gebruikersaccount controleren en configureren.Als Ouderlijk toezicht is ingeschakeld, kunt u de geselecteerde leeftijdscategorie en de status van het ouderlijk toezicht weergeven (dit wordt verder beschreven).

Ouderlijk beheer configureren voor een specifieke gebruikersaccount:

1. Gebruik de schakelaar om Ouderlijk toezicht voor die gebruikersaccount in te schakelen.
2. Stel de leeftijd van uw kind in door te klikken in het vak dat overeenkomt met de optie **Leeftijd**.Wanneer u de leeftijd van het kind instelt, worden de instellingen die voor die leeftijdscategorie als geschikt worden beschouwd, automatisch geladen volgens de ontwikkelingsnormen van het kind.
3. Klik op **Instellingen** als u de instellingen voor Ouderlijk toezicht in detail wilt configureren.Klik op een tabblad om de overeenkomende functie van Ouderlijk toezicht te configureren:
   - **Web** - hiermee kunt u de webnavigatie filteren en tijdbeperkingen op internettoegang instellen met Webbeheer.
   - **Toepassingen** - hiermee kunt u Toepassingsbeheer configureren om specifieke toepassingen te blokkeren of de toegang tot toepassingen te beperken.
   - **Trefwoorden** - hiermee kunt u de toegang tot het web, e-mails en instant messaging filteren met Trefwoordenbeheer.
   - **Instant messaging** - voor het configureren van Instant messaging beheer om chats met specifieke IM-contactpersonen via Yahoo! Messenger en Windows Live (MSN) Messenger toe te staan of te blokkeren.
   - **Categorieën** - om specifieke categorieën van webinhoud te blokkeren met de Categoriefilter.

   Om het venster met de instellingen voor Ouderlijk toezicht te sluiten, klikt u in de rechterbovenhoek op de X.De instellingen die u hebt geconfigureerd worden automatisch opgeslagen.

Ga naar het tabblad **Instellingen** om de opties voor de activiteitbewaking en Ouderlijk toezicht op afstand te configureren.De bewakingsopties naar wens configureren:

Activiteitenverslagen verzenden per e-mail
Telkens wanneer Ouderlijk toezicht van Bitdefender een activiteit blokkeert, wordt een e-mailmelding verzonden.U moet eerst de meldingsinstellingen configureren.

Een logboek voor internetverkeer opslaan
Registreert de websites die zijn bezocht door gebruikers waarvoor Ouderlijk toezicht is ingeschakeld.

Meer informatie vindt u onder “*De activiteit van de kinderen bewaken*” (p. 90).

Als u de computer en internetactiviteiten van uw kinderen op afstand wilt bewaken en controleren, schakelt u Ouderlijk toezicht op afstand in via de schakelaar.Meer informatie vindt u onder “*Ouderlijk toezicht op afstand*” (p. 92).

8.1.1. Webbeheer

Webbeheer helpt u bij het blokkeren van websites met ongepaste inhoud en het instellen van tijdbeperkingen voor internettoegang.

Webbeheer configureren voor een specifieke gebruikersaccount:

1. Open het venster met de instellingen voor Ouderlijk toezicht van Bitdefender voor die gebruikersaccount.
2. Klik op het tabblad **Web**.
3. Gebruik de schakelaar om Webbeheer in te schakelen.
4. Als u dat wilt, kunt u uw eigen regels maken om de toegang tot specifieke websites toe te staan of te blokkeren.Als Ouderlijk toezicht de toegang tot een website automatisch blokkeert, kunt u een regel maken om de toegang tot die website expliciet toe te laten.
5. U kunt limieten instellen op de tijd die uw kind kan doorbrengen op internet.Meer informatie vindt u onder “Internettoegang beperken op tijd” (p. 85).

Regels voor webbeheer maken

Volg deze stappen om de toegang tot een website toe te staan of te blokkeren:

1. Klik op **Website toestaan** of **Website blokkeren**.
2. Voer het websiteadres in het veld **Website** in.
3. Selecteer de gewenste actie voor deze regel - **Toestaan** of **Blokkeren**.
4. Klik op **Voltooien** om de regel toe te voegen.

Regels voor webbeheer beheren

De regels voor Websitebeheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. Het websiteadres en de huidige status worden weergegeven voor elke regel van het Webbeheer.

Om een regel te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

Om een regel te bewerken, dubbelklikt u erop (of selecteert u de regel en klikt u op **Bewerken**).Voer de nodige wijzigingen uit in het configuratievenster.

Internettoegang beperken op tijd

In het gebied Planning webtoegang, kunt u limieten instellen voor de tijd die uw kind mag doorbrengen op internet.

Selecteer **Webtoegang blokkeren** om de toegang tot het internet volledig te blokkeren.

Internettoegang beperken tot bepaalde perioden van de dag:

1. Selecteer **Webtijdbeperking**.
2. Click **Planning wijzigen**.
3. Selecteer de tijdsintervallen in het rooster voor het blokkeren van de internettoegang.U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken.Om een nieuwe selectie te starten, klikt u op **Alles blokkeren** of **Alles toestaan**.
4. Klik op **Opslaan**.

Opmerking

Bitdefender zal elk uur een update uitvoeren, ongeacht of de webtoegang is geblokkeerd.

8.1.2. Toepassingsbeheer

Het **Toepassingsbeheer** helpt u het uitvoeren van toepassingen te blokkeren. Games, media en messaging software, maar ook andere categorieën van software en malware kunnen op deze manier worden geblokkeerd. Toepassingen die op deze manier worden geblokkeerd, worden ook beschermd tegen wijzigingen en kunnen niet worden gekopieerd of verplaatst.U kunt toepassingen permanent of alleen gedurende bepaalde tijdsintervallen blokkeren, bijvoorbeeld wanneer uw kinderen hun huiswerk zouden moeten doen.

Toepassingsbeheer configureren voor een specifieke gebruikersaccount:

1. Open het venster met de instellingen voor Ouderlijk toezicht van Bitdefender voor die gebruikersaccount.
2. Klik op het tabblad **Toepassingen**.

3. Gebruik de schakelaar om Toepassingsbeheer in te schakelen.
4. Maak regels voor de toepassingen waarvoor u de toegang wilt blokkeren of beperken.

Regels voor Toepassingsbeheer maken

Volg deze stappen om de toegang tot een toepassing te blokkeren of te beperken:

1. Klik op **Blokkeren** of **Beperken**.
2. Klik op **Bladeren** om de toepassing waarvoor u de toegang wilt blokkeren/beperken te zoeken.Geïnstalleerde toepassingen bevinden zich doorgaans in de map `C:\Program Files`.
3. Selecteer de regelactie:
   - **Permanent blokkeren** om de toegang tot de toepassing volledig te blokkeren.
   - **Blokkeren op basis van deze planning** voor het beperken van de toegang tot bepaalde tijdsintervallen.

   Als u ervoor kiest de toegang te beperken in plaats van de toepassing volledig te blokkeren, moet u ook de dagen en tijdintervallen voor het blokkeren van de toegang selecteren in het raster.U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken.Om een nieuwe selectie te starten, klikt u op **Alles blokkeren** of **Alles toestaan**.
4. Klik op **Opslaan** om de regel toe te voegen.

Regels voor toepassingsbeheer beheren

De regels voor Toegangsbeheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. De naam van de toepassing, het pad en de huidige status worden weergegeven voor elke regel van het Toepassingsbeheer.

Om een regel te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

Om een regel te bewerken, dubbelklikt u erop (of selecteert u de regel en klikt u op **Bewerken**).Voer de nodige wijzigingen uit in het configuratievenster.

8.1.3. Beheer trefwoorden

Trefwoordenbeheer helpt u bij het blokkeren van de toegang van gebruikers tot e-mailberichten, webpagina's en instant messaging die specifieke woorden bevatten.Met Trefwoordenbeheer kunt u voorkomen dat kinderen ongepaste woorden en zinnen zien wanneer ze online zijn.Bovendien kunt u er zeker van zijn dat ze geen persoonlijke gegevens (zoals het thuisadres of het telefoonnummer) aan mensen die ze op internet ontmoeten geven.

Opmerking
Het trefwoordenbeheer voor instant messaging-toepassingen is alleen beschikbaar voor Yahoo Messenger en Windows Live (MSN) Messenger.

Trefwoordenbeheer configureren voor een specifieke gebruikersaccount:

1. Open het venster met de instellingen voor Ouderlijk toezicht van Bitdefender voor die gebruikersaccount.
2. Klik op het tabblad **Trefwoorden**.
3. Gebruik de schakelaar om Trefwoordenbeheer in te schakelen.
4. Regels voor trefwoordenbeheer aanmaken om te voorkomen dat ongepaste woorden worden weergegeven of belangrijke informatie wordt verzonden.

Regels voor het trefwoordenbeheer maken

Volg deze stappen om een woord of zin te blokkeren:

1. Klik op **Trefwoord blokkeren**.
2. Stel trefwoordinformatie in.
   - **Categorie trefwoorden** - voer de naam van de regel in dit veld in.
   - **Trefwoord** - voer het woord dat of de zin die u wilt blokkeren in het veld in.Indien u uitsluitend hele woorden wilt laten detecteren, selecteert u de checkbox **Overeenkomstig hele woorden**.
3. Selecteer het filtertype.
   - **Weergave blokkeren** - selecteer deze optie voor regels die zijn gemaakt om te verhinderen dat ongepaste woorden worden weergegeven.
   - **Verzending blokkeren** - selecteer deze optie voor regels die zijn aangemaakt om het verzenden van belangrijke informatie te voorkomen.
4. Selecteer het verkeerstype waarin Bitdefender moet scannen op het opgegeven woord.

Optie	Beschrijving
Web	Webpagina's die het trefwoord bevatten, worden geblokkeerd.
E-mail	E-mailberichten die het trefwoord bevatten, worden geblokkeerd.
Instant Messaging	Instant messages die het trefwoord bevatten, worden geblokkeerd.

5. Klik op **Voltooien** om de regel toe te voegen.

Vanaf nu zal elke poging tot het verzenden van de opgegeven gegevens (via e-mail, expresberichten of een webpagina) mislukken. Er verschijnt een waarschuwingsbericht met de melding dat Bitdefender het verzenden van identiteitsspecifieke inhoud heeft geblokkeerd.

Regels beheren voor trefwoordenbeheer

De regels voor Trefwoordenbeheer die zijn geconfigureerd, worden weergegeven in de tabel. Voor elke regel is gedetailleerde informatie voorzien.

Om een regel te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

Om een regel te bewerken, dubbelklikt u erop (of selecteert u de regel en klikt u op **Bewerken**).Voer de nodige wijzigingen uit in het configuratievenster.

8.1.4. Instant Messaging beheer

Met Instant Messaging (IM) beheer kan u de IM contacten aangeven waarmee uw kinderen mogen chatten.

Opmerking

IM beheer is alleen beschikbaar voor Yahoo Messenger en Windows Live (MSN) Messenger.

IM-beheer configureren voor een specifieke gebruikersaccount:

1. Open het venster met de instellingen voor Ouderlijk toezicht van Bitdefender voor die gebruikersaccount.
2. Klik op het tabblad **Instant Messaging**.
3. Gebruik de schakelaar om Beheer van expresberichten in te schakelen.
4. Selecteer de filtermethode van uw voorkeur en maak de beschikte regels afhankelijk van uw keuze.
   - **IM toestaan met alle contactpersonen, behalve de personen in de lijst**

     In dit geval moet u de IM-ID's (mensen waarmee uw kind niet mag praten) opgeven die u wilt blokkeren.
   - **IM blokkeren met alle contactpersonen, behalve de personen in de lijst**

     In dit geval moet u de IM-ID's opgeven waarmee uw kind expliciet expresberichten kan uitwisselen.U kunt bijvoorbeeld expresberichten toestaan met familieleden, schoolvrienden of buren.

     Deze tweede optie is aanbevolen als uw kind jonger is dan 14 jaar.

Regels voor het beheer van Instant messaging maken

Volg deze stappen om instant messaging met een contactpersoon toe te staan of te blokkeren:

1. Klik op **IM-ID blokkeren** of **IM-ID toestaan**.
2. Voer het e-mailadres of de gebruikersnaam die door de IM-contactpersoon wordt gebruikt in het veld **E-mail of IM-ID** in.
3. Kies het IM programma dat het contact gebruikt.
4. Selecteer de gewenste actie voor deze regel - **Toestaan** of **Blokkeren**.
5. Klik op **Voltooien** om de regel toe te voegen.

Regels voor het beheer van Instant messaging beheren

De regels voor IM-beheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster.

Om een regel te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

Om een regel te bewerken, dubbelklikt u erop (of selecteert u de regel en klikt u op **Bewerken**).Voer de nodige wijzigingen uit in het configuratievenster.

8.1.5. Categoriefilter

De Categoriefilter filtert de toegang tot websites op dynamische wijze volgens hun inhoud.Wanneer u Ouderlijk toezicht inschakelt en de leeftijd van uw kind instelt, wordt Categoriefilter automatisch geconfigureerd om websitecategorieën te blokkeren die als ongeschikt worden beschouwd voor de leeftijd van uw kind.Deze configuratie is geschikt in de meeste gevallen.

Als u meer controle wilt over de internetinhoud waaraan uw kind wordt blootgesteld, kunt u de specifieke websitecategorieën kiezen die moeten worden geblokkeerd door de Categoriefilter.

Volg deze stappen om de instellingen voor Categoriefilter voor een specifieke gebruikersaccount te controleren en te configureren:

1. Open het venster met de instellingen voor Ouderlijk toezicht van Bitdefender voor die gebruikersaccount.
2. Klik op het tabblad **Categorieën**.
3. Categoriecontrole is standaard ingeschakeld.Hoewel wij dit niet aanraden, kunt u ervoor kiezen om Categoriecontrole uit te schakelen en zelf een lijst van specifieke te blokkeren websites te configureren met Webbeheer.
4. U kunt controleren welke webcategorieën automatisch worden geblokkeerd/beperkt voor de momenteel geselecteerde leeftijdsgroep.Als de status van de categorie Zoekmachines **Geblokkeerd** is, zal uw kind geen enkele

zoekmachine mogen gebruiken.Als u niet tevreden bent met de standaardinstellingen, kunt u ze configureren zoals dat nodig is.

Om de actie die voor een specifieke categorie van webinhoud is geconfigureerd te wijzigen, klikt u op de huidige status en selecteert u de gewenste actie in het menu.

8.2. De activiteit van de kinderen bewaken

Bitdefender helpt u bij het volgen wat uw kinderen op de computer doen, zelfs als u niet thuis bent.

Wanneer Ouderlijk toezicht is ingeschakeld, worden de activiteiten van uw kinderen standaard geregistreerd. Zo kunt u altijd exact uitvinden welke websites ze hebben bezocht, welke toepassingen ze hebben gebruikt, welke activiteiten door Ouderlijk toezicht werden geblokkeerd, enz.

U kunt Bitdefender ook configureren om uw e-mailmeldingen te verzenden wanneer Ouderlijk toezicht een activiteit blokkeert.

8.2.1. De logboeken van Ouderlijk toezicht controleren

Open de logboeken van Ouderlijk toezicht om te controleren wat uw kinderen onlangs op de computer hebben gedaan.Volg deze stappen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Ouderlijk toezicht**.

Opmerking

Als u de computer niet deelt met uw kinderen, kunt u het Bitdefender-thuisnetwerk configureren zodat u op afstand toegang krijgt tot de logboeken van Ouderlijk toezicht (vanaf uw computer).Meer informatie vindt u onder “*Netwerk map*” (p. 107).

De logboek van Ouderlijk toezicht biedt gedetailleerde informatie over de computer en internetactiviteiten van uw kinderen.De informatie wordt geordend onder meerdere tabbladen:

Gebeurtenissen

Helpt u bij het zoeken van gedetailleerde informatie over de activiteiten van Ouderlijk toezicht (bijv. wanneer Ouderlijk toezicht werd in-/uitgeschakeld, welke gebeurtenissen werden geblokkeerd).

Klik op een gebeurtenis om details erover weer te geven.

Toepassingsgebruik

Helpt u bij het opsporen van de toepassingen die uw kinderen onlangs hebben gebruikt.

U kunt informatie filteren op gebruiker en op periode.Klik op een gebeurtenis om details erover weer te geven.

Internet Log

Helpt u bij het opsporen van de websites die uw kinderen onlangs hebben bezocht.

U kunt informatie filteren op gebruiker en op periode.Klik op een gebeurtenis om details erover weer te geven.

8.2.2. E-mailmeldingen configureren

Voor het ontvangen van e-mailmeldingen wanneer Ouderlijk toezicht een activiteit blokkeert:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Ouderlijk toezicht** en klik vervolgens op het tabblad **Instellingen**.
4. Schakel de optie **Activiteitenverslagen verzenden per e-mail** in met de overeenkomende schakelaar.
5. U wordt gevraagd de instellingen van uw e-mailaccount te configureren. Klik op **Ja** om het configuratievenster te openen.

   Opmerking

   U kunt het configuratievenster ook later openen door op **Meldingsinstellingen** te klikken.

6. Voer het e-mailadres in waarnaar de e-mailmeldingen moeten worden verzonden.
7. Configureer de e-mailinstellingen van de server die wordt gebruikt voor het verzenden van de e-mailmeldingen.Er zijn drie opties voor het configureren van de e-mailinstellingen:

   Gebruik de huidige mail-client-instellingen

   Deze optie is standaard geselecteerd wanneer Bitdefender de e-mailserverinstellingen van uw e-mailclient kan importeren.

   Selecteer van een van de bekende servers

   Selecteer deze optie als u een e-mailaccount hebt met een van de op het web gebaseerde e-mailservices in de lijst.

   Ik wil de serverinstellingen zelf configureren

   Als u de instellingen van de e-mailserver kent, selecteert u deze optie en configureert u de instellingen als volgt:

   - **Uitgaande SMTP-server** - typ het adres van de e-mailserver in die wordt gebruikt om e-mailberichten te verzenden.

- Als de server een andere poort dan de standaard poort 25 gebruikt, moet u het nummer in het overeenkomende veld invoeren.
- Als de server verificatie vereist, schakelt u het selectievakje **Mijn SMTP-server vereist verificatie** in en voert u uw gebruikersnaam en wachtwoord in de overeenkomende velden in.
- Als de server een door SSL beveiligde verbinding vereist, schakelt u het selectievakje **SSL gebruiken** in.

8. Klik op **Instellingen testen** om de instellingen te valideren. Als er tijdens de validatie problemen worden gevonden, wordt u op de hoogte gebracht van wat u moet doen om ze te corrigeren.
9. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

8.3. Ouderlijk toezicht op afstand

Met Ouderlijk toezicht op afstand kunt u de activiteiten van uw kinderen bewaken en de instellingen voor Ouderlijk toezicht wijzigen, zelfs als u niet thuis bent.U hebt alleen een computer met internettoegang en een webbrowser nodig.

Ouderlijk toezicht op afstand biedt een discrete manier om te controleren wat uw kinderen online doen, zonder te opdringerig te lijken.

8.3.1. Vereisten voor het gebruik van Ouderlijk toezicht op afstand

Om Ouderlijk toezicht op afstand te gebruiken, moet worden voldaan aan de volgende vereisten:

1. Installeer Bitdefender Internet Security 2012 of Bitdefender Total Security 2012 op de computer van uw kinderen.
2. Zorg dat u de productregistratie voltooit door uw product te koppelen aan een MyBitdefender-account.Meer informatie vindt u onder “*Productregistratie*” (p. 8).
3. Ouderlijk toezicht op afstand inschakelen.
4. De computer die u wilt gebruiken voor toegang tot Ouderlijk toezicht op afstand, moet met internet verbonden zijn.

8.3.2. Ouderlijk toezicht op afstand inschakelen

Ouderlijk toezicht op afstand inschakelen:

1. Meld u met een beheerdersaccount aan bij de computer waarop Bitdefender is geïnstalleerd.U kunt dezelfde account gebruiken die u hebt gebruikt voor het installeren van het programma.
2. Open het Bitdefender-venster.

3. Klik op de knop **Instellingen** in de werkbalk bovenaan.
4. Klik in het menu aan de linkerzijde op **Ouderlijk toezicht** en klik vervolgens op het tabblad **Instellingen**.
5. Schakel Ouderlijk toezicht op afstand in met de overeenkomende schakelaar.Ouderlijk toezicht op afstand zal worden ingeschakeld voor alle gebruikersaccounts op het systeem.

8.3.3. Ouderlijk toezicht op afstand openen

Ouderlijk toezicht op afstand is toegankelijk door aan te melden bij MyBitdefender.

1. Open een webbrowser op een computer met internettoegang en ga naar:

   https://my.bitdefender.com

2. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
3. Klik in het venster Services op **Hulp voor ouders** om toegang te krijgen tot het dashboard voor Ouderlijk toezicht op afstand.
4. U kunt alle computers zien waarop Ouderlijk toezicht op afstand is ingeschakeld, samen met hun overeenkomende gebruikersaccounts. Voor elke gebruikersaccount zijn er drie knoppen beschikbaar.
   - **Waarschuwingen** - om te controleren welke activiteiten werden geblokkeerd op de respectieve gebruikersaccount sinds uw laatste aanmelding.
   - **Activiteit** - om de recente activiteiten van uw kinderen te controleren.
   - **Instellingen** - om de instellingen voor Ouderlijk toezicht te wijzigen voor de respectieve gebruikersaccount.

   Wanneer u op een van deze knoppen klikt, wordt de pagina Ouderlijk toezicht op afstand van die gebruikersaccount geopend.

8.3.4. De activiteiten van uw kinderen op afstand bewaken

Voordat u de computer en internetactiviteiten van uw kinderen op afstand kunt bewaken, moet u Ouderlijk toezicht op afstand inschakelen op uw computer.Meer informatie vindt u onder “*Ouderlijk toezicht op afstand inschakelen*” (p. 92).

Op afstand controleren wat uw kinderen op hun computer doen:

1. Open een webbrowser op een computer met internettoegang en ga naar:

   https://my.bitdefender.com

2. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
3. Klik in het venster Services op **Hulp voor ouders** om toegang te krijgen tot het dashboard voor Ouderlijk toezicht op afstand.
4. Zoek de gebruikersaccount die uw kind gebruikt en klik op een van deze knoppen:

- **Waarschuwingen** - om te controleren welke activiteiten werden geblokkeerd op de respectieve gebruikersaccount sinds uw laatste aanmelding.
- **Activiteit** - om de recente activiteiten van uw kinderen te controleren.

Op de pagina Waarschuwingen kunt u zien welke websites, toepassingen of contactpersonen van expresberichten werden geblokkeerd sinds uw laatste aanmelding.Om een beperking te verwijderen, klikt u op de overeenkomende knop **Toestaan**.

Op de pagina Activiteit kunt u nuttige informatie terugvinden over de recente activiteiten van uw kinderen.

- die de meest geopende en de meest geblokkeerde websites zijn.
- die de meest geopende en de meest geblokkeerde toepassingen zijn.
- die de ID's van expresberichten zijn waarmee het meest contact werd opgenomen en die het meest werden geblokkeerd.

U kunt een website, een toepassing of een ID van expresberichten direct blokkeren door op de overeenkomende knop **Blokkeren** te klikken.

Om de weergegeven records te filteren, klikt u op het menu **Weergeven** en kiest u de gewenste optie.

8.3.5. De instellingen voor Ouderlijk toezicht op afstand wijzigen

Voordat u de instellingen voor Ouderlijk toezicht die u voor uw kinderen hebt geconfigureerd, op afstand kunt wijzigen, moet u Ouderlijk toezicht op afstand op hun computer inschakelen.Meer informatie vindt u onder *"Ouderlijk toezicht op afstand inschakelen"* (p. 92).

De instellingen voor Ouderlijk toezicht op afstand wijzigen:

1. Open een webbrowser op een computer met internettoegang en ga naar:

   https://my.bitdefender.com

2. Meld u aan bij uw Bitdefender-account met uw gebruikersnaam en wachtwoord.
3. Klik in het venster Services op **Hulp voor ouders** om toegang te krijgen tot het dashboard voor Ouderlijk toezicht op afstand.U kunt alle gebruikersaccounts zien waarvoor Ouderlijk toezicht op afstand is ingeschakeld.
4. Zoek de gebruikersaccount die uw kind gebruikt en klik op een van deze knoppen:
   - **Waarschuwingen** - om de lijst van recent geblokkeerde activiteiten te controleren en beperkingen te verwijderen.
   - **Activiteit** - om de recente activiteiten van uw kinderen te controleren en ongewenste activiteiten te blokkeren.

- **Instellingen** - om de instellingen voor Ouderlijk toezicht te wijzigen voor de respectieve gebruikersaccount.

5. Beperkingen naar wens instellen en verwijderen.

Internettoegang beperken op tijd

U kunt bepalen wanneer uw kind internettoegang krijgt via de opties van **Planning webtoegang** op de pagina **Instellingen**.

Internettoegang beperken tot bepaalde perioden van de dag:

1. Selecteer de tijdsintervallen in het rooster voor het blokkeren van de internettoegang.Om een nieuwe selectie te starten, klikt u op **Alles blokkeren** of **Alles toestaan**.
2. Klik op **Opslaan**.

Om de internettoegang volledig te blokkeren, klikt u op de koppeling **Alles blokkeren** onder het tijdraster en klikt u vervolgens op de koppeling **Opslaan**.

Wijzigingen zullen worden geconfigureerd en toegepast op de computer van uw kind na de volgende synchronisatie met de website Ouderlijk toezicht op afstand (binnen maximum 10 minuten).

Websites blokkeren

Een website blokkeren:

1. Ga naar de pagina **Instellingen**.
2. Geef de website op in het overeenkomende veld.
3. Klik op **Verzenden**.De website wordt toegevoegd aan de lijst van acties in behandeling.Als u uw mening verandert, klikt u op de overeenkomende knop **Actie annuleren**.

Opmerking

U kunt ook naar de pagina **Activiteit** gaan, de lijst van bezochte websites controleren en op de overeenkomende knop **Blokkeren** klikken wanneer u een website wilt blokkeren.

De regel wordt geconfigureerd en toegepast op de computer van uw kind na de volgende synchronisatie met de website Ouderlijk toezicht op afstand (binnen maximum 10 minuten).

IM-contactpersonen blokkeren

Expresberichten van/naar een specifieke contactpersoon blokkeren:

1. Ga naar de pagina **Instellingen**.
2. Voer de ID voor expresberichten in het overeenkomende veld in.

3. Klik op **Blokkeren**.De IM-ID wordt toegevoegd aan de lijst van acties in behandeling.Als u uw mening verandert, klikt u op de overeenkomende knop **Actie annuleren**.

Opmerking

U kunt ook naar de pagina **Activiteit** gaan, de lijst van IM-contactpersonen met wie uw kind heeft gechat controleren en op de overeenkomende knop **Blokkeren** klikken wanneer u een ongewenste contactpersoon vindt.

De regel wordt geconfigureerd en toegepast op de computer van uw kind na de volgende synchronisatie met de website Ouderlijk toezicht op afstand (binnen maximum 10 minuten).

Toepassingen blokkeren

Een toepassing blokkeren:

1. Ga naar de pagina **Activiteit**.
2. Controleer de lijst van geopend toepassingen en klik op de overeenkomende knop **Blokkeren** wanneer u een ongewenste toepassing vindt.

De regel wordt geconfigureerd en toegepast op de computer van uw kind na de volgende synchronisatie met de website Ouderlijk toezicht op afstand (binnen maximum 10 minuten).

De blokkering van websites, toepassingen of IM-contactpersonen opheffen

De pagina Waarschuwingen toont de websites, toepassingen en ID's van expresberichten die zijn geblokkeerd door Ouderlijk toezicht.Om een beperking te verwijderen, klikt u op de overeenkomende knop **Toestaan**.De beperking wordt verwijderd van de computer van uw kind na de volgende synchronisatie met de website Ouderlijk toezicht op afstand (binnen maximum 10 minuten).

9. Firewall

De Firewall beschermt uw computer tegen onbevoegde binnenkomende en uitgaande verbindingspogingen.Dit kan worden vergeleken met een wachter bij uw poort – de toepassing traceert verbindingspogingen en beslist welke moeten worden toegestaan en welke moeten worden geblokkeerd.

Opmerking
Een firewall is bijzonder belangrijk wanneer u een breedband- of DSL-verbinding hebt.

Als uw computer werkt met Windows Vista of Windows 7, wijst Bitdefender automatisch een netwerktype toe aan elke nieuwe netwerkverbinding die het detecteert.Op computers waarop Windows XP wordt uitgevoerd, wordt u gevraagd het type netwerk te selecteren.Meer informatie over de firewall-instellingen voor elk netwerktype en de manier waarop u de netwerkinstellingen kunt bewerken, vindt u onder “*De instellingen voor de netwerkverbinding configureren*” (p. 98).

De Bitdefender-firewall gebruikt een reeks regels om gegevens te filteren die naar en van uw systeem zijn overgedragen.De regels zijn gegroepeerd in 3 categorieën:

Algemene regels
: Regels die vastleggen via welke protocollen communicatie is toegelaten.

  Er wordt een standaard set met regels gebruikt die een optimale bescherming biedt.U kunt de regels bewerken door verbindingen via bepaalde protocollen toe te staan of te weigeren.

Toepassingsregels
: Regel die bepalen hoe elk toepassing toegang krijgt tot de netwerkbronnen en internet.

  In normale omstandigheden maakt Bitdefender automatisch een regel wanneer een toepassing toegang probeert te krijgen via internet.U kunt regels voor toepassingen ook handmatig toevoegen of bewerken.

Adapterregels
: Regels die bepalen of uw computer kan communiceren met bepaalde andere computers.

  U moet regels maken om verkeer specifiek toe te staan of te weigeren.

Er wordt aanvullende bescherming geboden door het Inbraakdetectiesysteem (IDS).Het inbraakdetectiesysteem bewaakt de netwerk- en systeemactiviteiten en beschermt ze tegen boosaardige activiteiten of overtredingen van het beleid.Niet alleen pogingen tot het wijzigen van kritieke systeembestanden, Bitdefender-bestanden of registergegevens, worden hiermee gedetecteerd en geblokkeerd, maar ook pogingen om malwarestuurprogramma’s te installeren en aanvallen door de injectie van codes (DLL-injectie) worden verhinderd.

9.1. De firewall-beveiliging in- of uitschakelen

Volg deze stappen om de firewallbescherming in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Ga naar het paneel **Firewall**.
3. Klik op de schakelaar Firewall.

Waarschuwing

Omdat het uw computer blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn.Schakel de firewall zo snel mogelijk opnieuw in.

9.2. De instellingen voor de netwerkverbinding configureren

Volg deze stappen om de netwerkverbindingsinstellingen weer te geven en te bewerken:

1. Open het Bitdefender-venster.
2. Ga naar het paneel **Firewall**.
3. Klik op **Netwerkdetails**.

Een nieuw venster wordt weergegeven.De grafiek bovenaan in het venster toont real time informatie over binnenkomend en uitgaand verkeer.

Onder de grafiek wordt de volgende informatie weergegeven voor elke netwerkverbinding.

- **Netwerktype** - het type netwerk waarmee de computer verbonden is.Bitdefender is van toepassing op een basisset firewall-instellingen, afhankelijk van het typte netwerk waarmee u verbonden bent.

  U kunt het type wijzigen door het vervolgkeuzemenu **Netwerktype** te openen en een van de beschikbare types in de lijst te selecteren.

Netwerktype	Beschrijving
Vertrouwd	De firewall voor de betreffende adapter uitschakelen.
Thuis/Bureau	Alle verkeer tussen uw computer en computers in het netwerk toestaan.
Openbaar	Alle verkeer blokkeren is uitgeschakeld.
Niet-vertrouwd	Netwerk- en internetverkeer door de betreffende adapter compleet blokkeren.

- **Stealth-modus** - hiermee kunt u instellen of u door andere computers kunt worden gedetecteerd.

  Om de Stealth-modus te configureren, klikt u op de pijl in de kolom **Stealth-modus** en selecteert u de gewenste optie.

Stealth-optie	Beschrijving
Aan	Stealth-modus is aan.Uw computer is zowel onzichtbaar vanaf het lokale netwerk als vanaf internet.
Uit	Stealth-modus is uit.Iemand op het lokale netwerk of het internet kan pingen en uw computer detecteren.
Remote	Uw computer kan niet gedetecteerd worden vanaf het internet.Lokale netwerk gebruikers kunnen pingen en uw computer detecteren.

- **Algemeen** - hiermee kunt u instellen of er generieke regels moeten worden toegepast op deze verbinding.

  Als het IP-adres van een netwerkadapter wordt gewijzigd, zal Bitdefender het netwerktype overeenkomstig wijzigen.Als u hetzelfde type wilt behouden, klikt u op de pijl in de kolom **Algemeen** en selecteert u **Ja**.

9.3. Inbraakdetectiesysteem

Volg deze stappen om het inbraakdetectiesysteem te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Instellingen**.
4. Om het inbraakdetectiesysteem in te schakelen, klikt u op de overeenkomende schakelaar.
5. Sleep de schuifregelaar langs de schaal om het gewenste agressiviteitsniveau in te stellen.Gebruik de beschrijving aan de rechterzijde van de schaal om het niveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

U kunt controleren welke toepassingen zijn gedetecteerd door het inbraakdetectiesysteem in het venster Gebeurtenissen.

Als er toepassingen zijn die u vertrouwt en niet wilt dat het inbraakdetectiesysteem scant, kunt u uitsluitingsregels toevoegen voor deze toepassingen.Volg de stappen

beschreven in *"Uitgesloten processen beheren"* (p. 59) om een toepassing uit te sluiten van de scan.

Opmerking

De werking van de inbraakdetectiesysteem is verwant met deze van Actief virusbeheer.Regels voor de uitsluiting van processen zijn van toepassing op beide systemen.

9.4. Verkeerinstellingen configureren

Volg deze stappen om verkeerinstellingen te configureren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Instellingen**.

De volgende functies kunnen worden ingeschakeld of uitgeschakeld in de sectie **Verkeer**.

- **ICS-ondersteuning (Internet Connection Sharing) inschakelen** - schakelt de ondersteuning in voor ICS (Internet Connection Sharing).

  Opmerking

  Met deze optie wordt ICS niet automatisch ingeschakeld op uw systeem, maar wordt dit type verbinding alleen toegestaan wanneer u het inschakelt via uw besturingssysteem.

- **Poort scans blokkeren** - detecteert en blokkeert pogingen om uit te vinden welke poorten open zijn.

  Poortscans worden vaak door hackers gebruikt om geopende poorten op uw computer te vinden.Als zij een minder veilige of kwetsbare poort vinden kunnen zij inbreken in uw computer.

- **Meer logboekinformatie** - vermeerdert de informatie van het firewall-logboek.

  Bitdefender houdt een logboek bij van gebeurtenissen met betrekking tot het gebruik van de Firewall-module (in-/uitschakelen firewall, blokkeren van verkeer, wijzigen van instellingen) of een lijst die is gegenereerd door activiteiten die door deze module zijn gedetecteerd (scannen van poorten, blokkeren van verbindingspogingen of verkeer volgens de regels).Het logboek is toegankelijk vanaf het venster **Firewall-activiteit** door op **Logboek weergeven** te klikken.Het logboekbestand kunt u vinden onder `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

- **WiFi-meldingen weergeven** - als u verbonden bent met een draadloos netwerk, worden informatievensters weergegeven met betrekking tot specifieke

netwerkgebeurtenissen (bijvoorbeeld, wanneer een nieuwe computer bij het netwerk is gekomen).

9.5. Algemene regels

Telkens wanneer gegevens via internet worden verzonden, worden bepaalde protocollen gebruikt.

Via de algemene regels kunt u configureren via welke protocollen verkeer is toegestaan.Volg deze stappen om de regels te bewerken:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Firewallregels op **Algemene regels**.

Een nieuw venster wordt weergegeven.De huidige regels worden weergegeven.

Om een regel te bewerken, klikt u op de overeenkomende pijl in de kolom **Actie** en selecteert u **Toestaan** of **Weigeren**.

DNS via UDP/TCP
DNS via UDP en TCP toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

Binnenkomende ICMP/ICMPv6
ICMP-/ ICMPv6-berichten toestaan of weigeren.

ICMP-berichten worden vaak gebruikt door hackers om aanvallen op computernetwerken uit te voeren.Dit type verbinding wordt standaard geweigerd.

E-mails verzenden
Het verzenden van e-mails via SMTP toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

HTTP webbrowsing
HTTP surfen op het web toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

Inkomende desktopverbindingen op afstand
Toegang van andere computers via verbindingen met extern bureaublad toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

Windows Verkenner-verkeer op HTTP/FTP
HTTP- en FTP-verkeer van Windows Verkenner toestaan of weigeren.

Dit type verbinding wordt standaard geweigerd.

9.6. Toepassingsregels

Klik op **Toepassingsregels** om de firewallregels die de toegang bepalen van de toepassingen tot netwerkbronnen en internet, te beheren.

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Firewallregels op **Toepassingsregels**.

U kunt de programma's (processen) zien waarvoor er firewallregels zijn gemaakt in de tabel.Om de regels voor een specifieke toepassing te zien, klikt u op het vakje + naast de betreffende toepassing of dubbelklikt u erop.

Voor elke regel wordt de volgende informatie weergegeven:

- **Proces/Netwerktypen** - het proces en de netwerkadaptertypes waarop de regel van toepassing is.Regels zijn automatisch gecreëerd voor het filteren van netwerk- of internettoegang via elke adapter.U kan handmatig regels creëren of bewerken voor het filteren van de netwerk- of internettoegang van een applicatie via een specifieke adapter (bijvoorbeeld een draadloze netwerkadapter)
- **Protocol** - het IP-protocol waarvoor de regel geldt.U kan een van de volgende dingen zien:

Protocol	Beschrijving
Alle	Omvat alle IP-protocollen.
TCP	Transmission Control Protocol - TCP activeert twee hosts om een verbinding tot stand te brengen en gegevensstromen uit te wisselen. TCP garandeert het afleveren van gegevens en verzekert eveneens dat de pakketten worden afgeleverd in dezelfde volgorde waarin ze worden verzonden.
UDP	User Datagram Protocol - UDP is een transport gebaseerd op IP en ontwikkeld voor hoge prestaties. Games en andere op video gebaseerde toepassingen gebruiken vaak UDP.
Een getal	Geeft een specifiek IP-protocol aan (ander dan TCP en UDP).U vindt de complete lijst van toegewezen IP-protocolnummers op http://www.iana.org/assignments/protocol-numbers.

- **Actie** - of de toepassing al dan niet netwerk- of internettoegang krijgt onder de opgegeven omstandigheden.

Gebruik de knoppen in het onderste deel van het venster voor het beheren van de regels.

- **Regel toevoegen** - opent het venster Toepassingsregel toevoegen waarin u een nieuwe regel kunt maken.
- **Regel bewerken** - opent het venster Toepassingsregel bewerken waar u de instellingen van een geselecteerde regel kunt wijzigen.
- **Regel verwijderen** - verwijdert de geselecteerde regel.

Toepassingsregels toevoegen/bewerken

Klik op de overeenkomende knop om een regel toe te voegen of te bewerken.Een nieuw venster wordt weergegeven. Ga als volgt te werk:

- **Programmapad.** Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt.
- **Lokaal adres.** Specify the local IP address and port the rule applies to.Als u meer dan een netwerkadapter hebt, kunt u het selectievakje **Elke** uitschakelen en een specifiek IP-adres invoeren.
- **Adres op afstand.** Specify the remote IP address and port the rule applies to.Om het verkeer te filteren tussen uw computer en een specifieke computer, schakelt u het selectievlakje **Alle** uit en typt u u het IP-adres.
- **Netwerktype.** Selecteer het type netwerk waarvoor de regel geldt.
- **Gebeurtenissen.** Afhankelijk van het geselecteerde protocol, selecteert u de netwerkgebeurtenissen waarop de regel geldt.De volgende gebeurtenissen kunnen verwerkt worden:

Gebeurtenis	Beschrijving
Verbinden	Voor-uitwisseling van standaardberichten die worden gebruikt door verbinding-georienteerde protocollen (zoals TCP) om een verbinding tot stand te brengen.Met connectie-georienteerde protocollen, vindt dataverkeer tussen twee computers alleen plaats nadat een verbinding tot stand is gebracht.
Verkeer	Datastroom tussen twee computers.
Luisteren	Staat waarin een applicatie het netwerk bewaakt in afwachting van het tot stand brengen van een verbinding of voor het ontvangen van informatie van en peer applicatie.

- **Protocol.** Selecteer in het menu het IP-protocol waarvoor de regel geldt.
  - ▶ Als u een regel voor alle protocollen wilt laten gelden, schakelt u het selectievakje **Alle** in.

- Als u wilt dat de regel van toepassing is op TCP, selecteert u **TCP**.
- Als u wilt dat de regel van toepassing is op UDP, selecteert u **UDP**.
- Als u een regel voor specifiek protocol wilt laten gelden, schakelt u het selectievakje **Andere** in.Een bewerkingsveld verschijnt.Typ het nummer dat is toegewezen aan het protocol dat u wilt filteren in het bewerkingsveld.

Opmerking

IP-protocolnummers worden toegewezen door de Internet Assigned Numbers Authority (IANA).U vindt de complete lijst van toegewezen IP-protocolnummers op http://www.iana.org/assignments/protocol-numbers.

- **Richting.** Selecteer in het menu de verkeersrichting waarvoor de regel geldt.

Richting	Beschrijving
Uitgaand	De regel zal alleen voor uitgaand verkeer worden toegepast.
Inkomend	De regel zal alleen voor inkomend verkeer worden toegepast.
Beide	De regel zal in beide richtingen worden toegepast.

- **IP-versie.** Selecteer in het menu de IP-versie (IPv4, IPv6 of alle) waarvoor de regel geldt.
- **Machtiging.** Selecteer een van de beschikbare machtigingen:

Machtiging	Beschrijving
Toestaan	De opgegeven toepassing zal netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.
Weigeren	De opgegeven toepassing zal geen netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.

9.7. Adapterregels

Voor elke netwerkverbinding kunt u speciale vertrouwde of niet-vertrouwde zones configureren.

Een vertrouwde zone is een apparaat dat u volledig vertrouwt, bijv. een computer of een printer.Al het verkeer tussen uw computer en een vertrouwd apparaat is toegestaan.Om bronnen te delen met specifieke computers in een onbeveiligd draadloos netwerk, voegt u ze toe als toegestane computers.

Een niet-vertrouwde zone is een apparaat dat u helemaal niet met uw computer wilt laten communiceren.

Volg deze stappen om gebieden op uw netwerkadapters weer te geven en te beheren:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Firewallregels op **Adapterregels**.

Een nieuw venster wordt weergegeven.De huidige netwerkzones worden weergegeven per adapter.

Gebruik de knoppen in het bovenste deel van het venster voor het beheren van de zones.

- **Zone toevoegen** - opent het venster IP-adres toevoegen waarin u een nieuwe zone voor een geselecteerde adapter kunt maken.
- **Zone bewerken** - opent het venster Regel bewerken waar u de instellingen van een geselecteerde zone kunt wijzigen.
- **Zone verwijderen** - verwijdert de geselecteerde zone.

Zones toevoegen / bewerken

Klik op de overeenkomende knop om een zone toe te voegen of te bewerken.Er wordt een nieuw venster weergegeven met de IP-adressen van de apparaten die met het netwerk zijn verbonden.Ga als volgt te werk:

1. Selecteer het IP-adres van de computer die u wilt toevoegen of voer een adres of adresbereik in het opgegeven tekstvak in.
2. De actie selecteren:
   - **Toestaanscannen** - om alle verkeer tussen uw computer en de geselecteerde computer toe te staan.
   - **Verbieden** - om alle verkeer tussen uw computer en de geselecteerde computer te blokkeren.
3. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

9.8. De netwerkactiviteit bewaken

Om de huidige netwerk-/internetactiviteit (via TCP en UDP) gesorteerd op toepassing te bewaken en het Bitdefender Firewall-logboek te openen, volgt u de onderstaande stappen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Netwerkactiviteit op **Firewall-activiteit**.

Een nieuw venster wordt weergegeven.U kunt alle verkeer, gesorteerd op toepassing, zien. Voor elke toepassing ziet u de verbindingen en open poorten, evenals de statistieken met betrekking tot de snelheid van het uitgaande & binnenkomende verkeer en de totale hoeveelheid verzonden/ontvangen gegevens.

Naast elke verbinding wordt een pictogram weergegeven.De pictogrammen betekenen:

- Geeft een uitgaande verbinding aan.
- Geeft een binnenkomende verbinding aan.
- Geeft een open poort op uw computer aan.

Het venster toont de huidige netwerk-/internetactiviteit in real time. Wanneer de verbinding of poorten worden gesloten, ziet u dat de overeenkomende statistieken worden gedimd en, na verloop van tijd, verdwijnen.Hetzelfde gebeurt met alle statistieken die overeenkomen met een toepassing die verkeer genereert of open poorten heeft en die u sluit.

Voor een uitgebreide lijst van gebeurtenissen met betrekking tot het gebruik van de Firewall-module (in-/uitschakelen firewall, blokkeren van verkeer, wijzigen van instellingen) of een lijst die is gegenereerd door activiteiten die door deze module zijn gedetecteerd (scannen van poorten, blokkeren van verbindingspogingen of verkeer volgens de regels), kunt u het Firewall-logboek van Bitdefender weergeven door op **Logboek weergeven** te klikken.

10. Netwerk map

Met de Netwerkmodule kan u de Bitdefender producten die zijn geïnstalleerd op uw thuiscomputers beheren vanaf één enkele computer.

Volg deze stappen om de Bitdefender producten die zijn geïnstalleerd op uw computer te beheren:

1. Schakel het Bitdefender-netwerk in op uw computer.Stel uw computer in als **servercomputer**.
2. Naar elke computer gaan die u wilt beheren en koppelen aan het netwerk (wachtwoord instellen)Stel elke computer in als **Standaardcomputer**.
3. Naar uw computer teruggaan en de computers toevoegen die u wilt beheren.

10.1. Het Bitdefender-netwerk inschakelen

Volg deze stappen om het Bitdefender-netwerk in te schakelen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Netwerkmap**.
4. Klik op **Netwerk inschakelen**.U wordt gevraagd het beheerwachtwoord voor de netwerkmap te configureren.
5. Voer hetzelfde wachtwoord in elk van de bewerkingsvelden in.
6. Stel de rol in van de computer in de Bitdefender-netwerkmap in:
   - **Servercomputer** - selecteer deze optie op de computer die zal worden gebruikt voor het beheren van alle andere.
   - **Standaardcomputer** - selecteer deze optie op computers die zullen worden beheerd door de servercomputer.
7. Klik op **OK**.

   U ziet de naam van de computer in de netwerkmap.

   De knop **Verbinding uitschakelen** verschijnt.

Opmerking

U kunt de netwerkmap ook inschakelen vanaf het hoofdvenster van Bitdefender:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Netwerkmap**.
3. Klik op **Beheren** en selecteer **Netwerk inschakelen** in het vervolgkeuzemenu.

10.2. Computers toevoegen aan het Bitdefender-netwerk

Elke computer wordt automatisch toegevoegd aan het netwerk als het voldoet aan de volgende criteria.

- de Bitdefender-netwerkmap is erop ingeschakeld.
- de rol werd ingesteld op Standaardcomputer.
- Het wachtwoord dat wordt ingesteld wanneer het netwerk wordt ingeschakeld, is hetzelfde als het wachtwoord dat is ingesteld op de servercomputer.

Opmerking

U kunt de netwerkmap op elk ogenblik scannen op computers die voldoen aan de criteria door op de knop **Automatisch opsporen** te klikken.

Volg de onderstaande stappen om een computer toe te voegen aan de Bitdefender-netwerkmap vanaf de servercomputer:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Netwerkmap**.
4. Klik op **Computer toevoegen**.
5. Typ het beheerwachtwoord en klik op **OK**.Een nieuw venster wordt weergegeven.

   U ziet de lijst van computers in het netwerk.Het pictogram betekent:

    Een online computer zonder Bitdefender producten.

    Een online computer met Bitdefender producten.

    Een offline computer met Bitdefender producten.
6. U kunt een van de volgende methoden gebruiken:
   - In de lijst de naam van de toe te voegen computer selecteren.
   - Het IP-adres of de naam van de comuter in het overeenkomende veld invoeren.
7. Klik op **Toevoegen**.
8. Voer het beheerwachtwoord in dat is geconfigureerd op de betreffende computer.
9. Klik op **OK**.Als het correcte wachtwoord is ingevoerd, verschijnt de naam van de geselecteerde computer in de netwerkmap.

10.3. Het Bitdefender-netwerk beheren

Als met succes een Bitdefender-netwerkmap is gemaakt, Bitdefender-producten beheren vanaf de servercomputer.

Volg de onderstaande stappen om meerdere taken uit te voeren op alle beheerde computers:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Netwerkmap**.
3. Klik op **Beheren** en selecteer de overeenkomende knoppen via het vervolgkeuzemenu.
   - **Verbinding uitschakelen** - hiermee kunt u het netwerk uitschakelen.
   - **Alles scannen** - hiermee kan u alle beheerde computers tegelijk scannen.
   - **Alles updaten** - hiermee kan u alle beheerde computers tegelijk updaten.

Voordat u een taak op een specifieke computer kan uitvoeren, moet u het lokale beheerwachtwoord invoeren.Typ het beheerwachtwoord en klik op **OK**.

Volg deze stappen om de volledige netwerkmap te zien en toegang te krijgen tot alle beheertaken:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Netwerkmap**.

Als u de muiscursor boven een computer in de netwerkmap plaatst, ziet u korte informatie ervan (IP-adres, aantal problemen dat de systeemveiligheid bedreigt, registratiestatus Bitdefender).

Als u klikt op een computernaam in de netwerkmap, ziet u alle administratieve taken die u op de externe computer kunt uitvoeren.

Product registreren
Hiermee kunt u Bitdefender op deze computer registreren door een licentiesleutel in te voeren.

Wachtwoord voor productinstellingen configureren
Hiermee kunt u een wachtwoord maken om de toegang tot de Bitdefender-instellingen op deze pc te beperken.

Een scantaak op aanvraag uitvoeren
Hiermee kunt u een scan op aanvraag maken op de externe computer. U kunt elk van de volgende scantaken uitvoeren: Snelle scan of Volledige systeemscan.

Herstellen
Hiermee kunt u de problemen die de veiligheid van uw computer beïnvloeden oplossen door de wizard Alle problemen oplossen te volgen.

Gebeurtenissen tonen
Hiermee krijgt u toegang tot de module **Gebeurtenissen** van het Bitdefender-product dat op deze computer is geïnstalleerd.

Nu bijwerken
Start het updateproces voor het Bitdefender-product dat op deze computer is geïnstalleerd.

Het profiel voor Ouderlijk toezicht instellen

Hiermee kunt u de leeftijdscategorie instellen die moet worden gebruikt door de webfilter Ouderlijk toezicht op deze computer.

Instellen als updateserver voor dit netwerk

Hiermee kunt u deze computer instellen als de updateserver voor alle Bitdefender-producten die op de computers in dit netwerk zijn geïnstalleerd.Het gebruik van deze optie zal het internetverkeer beperken omdat slechts één computer in het netwerk een verbinding zal maken met internet om updates te downloaden.

PC verwijderen uit netwerkmap

Hiermee kunt u een pc uit het netwerk verwijderen.

Opmerking

Als u verschillende taken wilt uitvoeren, kan u het selectievakje **Dit bericht niet weergeven tijdens deze sessie** inschakelen.Als u deze optie selecteert, wordt u tijdens de huidige sessie niet opnieuw naar het wachtwoord gevraagd.

11. Update

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u Bitdefender up-to-date houdt met de meest recente malware handtekeningen.

Als u via breedband of DSL verbonden bent met het Internet, zal Bitdefender deze taak op zich nemen. Het programma controleert standaard op updates wanneer u uw computer inschakelt en daarna ieder **uur**.Als er een update is gedetecteerd, wordt deze automatisch gedownload en geïnstalleerd op uw computer.

Het updateproces wordt "on the fly" uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

Belangrijk

Houd Automatische update ingeschakeld om u te beschermen tegen de laatste bedreigingen.

In sommige specifieke situaties is uw tussenkomst vereist om de bescherming van uw Bitdefender up-to-date te houden:

- Als uw computer een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in "*Bitdefender configureren voor het gebruik van een proxy-internetverbinding*" (p. 37).
- Als u geen internetverbinding hebt, kunt u Bitdefender handmatig bijwerken zoals beschreven in "*Mijn computer is niet verbonden met internet. Bitdefender bijwerken*" (p. 122).Het handmatige updatebestand wordt eenmaal per week uitgegeven.
- Er kunnen fouten optreden tijdens het downloaden van updates bij een trage internetverbinding.Raadpleeg "*Bitdefender updaten bij een langzame internetverbinding*" (p. 122) voor meer informatie over het oplossen van dergelijke fouten.
- Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten.Meer informatie vindt u onder "*Een update uitvoeren*" (p. 112).

11.1. Controleren of Bitdefender up-to-date is

Volg deze stappen om te controleren of uw Bitdefender-bescherming up-to-date is:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Update**.

3. Het tijdstip van de laatste update wordt net onder de naam van het venster weergegeven.

Controleer de updategebeurtenissen voor gedetailleerde informatie over de laatste updates:

1. Klik in het hoofdvenster op **Gebeurtenissen** in de werkbalk bovenaan.
2. Klik in het menu aan de linkerzijde op **Update**.

U kunt uitzoeken wanneer updates werden gestart en u kunt informatie over de updates weergeven (of ze al dan niet gelukt zijn, of het opnieuw opstarten is vereist om de installatie te voltooien, enz.);Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

11.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

Voer een van de volgende bewerkingen uit om een update te starten:

- Open het Bitdefender-venster, ga naar het deelvenster **Update** en klik op **Nu bijwerken**.
- Klik met de rechtermuisknop op het Bitdefender-pictogram in het systeemvak en selecteer **Nu bijwerken**.

De module Update maakt een verbinding met de updateserver van Bitdefender en controleert op updates.Als een update is gedetecteerd, wordt u gevraagd de update te bevestigen, of wordt de update automatisch uitgevoerd, afhankelijk van de Update-instellingen.

Belangrijk

Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.

11.3. De automatische update in- of uitschakelen

Volg deze stappen om de automatische update in of uit te schakelen:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Update**.
3. Klik op de schakelaar om Automatische Update in of uit te schakelen.
4. Als u de automatische update wilt uitschakelen, verschijnt een waarschuwingsvenster.U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kan de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, permanent of tot het systeem opnieuw wordt opgestart.

Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij adviseren de automatische update zo kort mogelijk uit te schakelen. Als Bitdefender niet regelmatig wordt geüpdatet, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

11.4. De update-instellingen aanpassen

De updates kunnen worden uitgevoerd vanaf het lokale netwerk, via het Internet, rechtstreeks of via een proxyserver.Bitdefender zal standaard elk uur via het internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

De standaardinstellingen voor de update zijn geschikt voor de meeste gebruikers en u hoeft ze normaal niet te wijzigen.

Volg deze stappen om de update-instellingen te wijzigen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Update**.
4. Pas de instellingen aan volgens uw voorkeur.

Update-locatie

Bitdefender is geconfigureerd om een update uit te voeren vanaf de Bitdefender-updateservers op internet.De updatelocatie is `http://upgrade.bitdefender.com`, een algemeen internetadres dat automatisch wordt omgeleid naar dichtstbijzijnde Bitdefender-updateserver in uw regio.

Wijzig de updatelocatie niet tenzij u dit wordt aangeraden door een Bitdefender-vertegenwoordiger of door uw netwerkbeheerder (als u verbonden bent met een kantoornetwerk).

Als u Bitdefender hebt geïnstalleerd op verschillende computers in uw gezin, kunt u een Bitdefender-thuisnetwerk instellen en vervolgens een van uw computers aanduiden als de updateserver.Meer gedetailleerde informatie vindt u in “*Netwerk map*” (p. 107).Het Bitdefender-programma dat op de aangewezen updateserver is geïnstalleerd, wordt bijgewerkt vanaf internet. De Bitdefender-programma’s op de andere computers zullen hun updates krijgen van de lokale updateserver (hun updatelocatie wordt automatisch overeenkomend gewijzigd).Deze configuratie is bedoeld om internetverkeer te minimaliseren en updates te optimaliseren.

U kunt terugkeren naar de algemene locatie voor internetupdates door op **Standaard** te klikken.

Regels voor behandelen updates

U hebt de keuze uit drie manieren voor het downloaden en installeren van de updates.

- **Stille update** - Bitdefender downloadt en installeert de update automatisch.
- **Herinneren voor het downloaden** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.
- **Herinneren voor het installeren** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

Voor sommige updates moet het systeem opnieuw worden opgestart om de installatie te voltooien.Als een update het opnieuw opstarten van het systeem vereist, blijft Bitdefender werken met de oude bestanden tot de gebruikers de computer opnieuw opstart. Hiermee wordt voorkomen dat de Bitdefender-update het werk van de gebruiker hinder.

Als u een vraag om bevestiging wilt wanneer een update het opnieuw opstarten van het systeem vereist, schakelt u de optie **Opnieuw opstarten uitstellen** uit door op de overeenkomende schakelaar te klikken.

P2P-updates

Naast het normale updatemechanisme, gebruikt Bitdefender ook een slim systeem voor het delen van updates, gebaseerd op een peer-to-peer-protocol (P2P) voor het distribueren van updates van malwarehandtekeningen tussen gebruikers van Bitdefender.

U kunt de opties voor de P2P-update in- of uitschakelen met de overeenkomende schakelaars.

P2P-update-systeem gebruiken
Schakel deze optie in voor het downloaden van updates van malwarehandtekeningen van andere Bitdefender-gebruikers die het P2P-updatesysteem gebruiken.Bitdefender gebruikt poorten 8880 - 8889 voor peer-to-peer update.

Bitdefender-bestanden distribueren
Schakel deze optie in om de nieuwste beschikbare malwarehandtekeningen op uw computer te delen met andere Bitdefender-gebruikers.

12. Safego-beveiliging voor sociale netwerken

U vertrouwt uw online vrienden.Maar vertrouwt u hun computers?Gebruik de Safego-beveiliging voor sociale netwerken om uw account en uw vrienden te beschermen tegen van online bedreigingen.

Safego is een Facebook-toepassing die is ontwikkeld door Bitdefender om uw sociale netwerkaccount veilig te houden.Deze module heeft de taak de koppelingen die u ontvangt van uw Facebook-vrienden te scannen en de privacy-instellingen van uw account te bewaken.

Opmerking
Er is een MyBitdefender-account vereist om deze functie te gebruiken.
Meer informatie vindt u onder “*Productregistratie*” (p. 8).

Dit zijn de hoofdfuncties:

- scant automatisch de publicaties in uw newsfeed op boosaardige koppelingen.
- beschermt uw account tegen online bedreigingen.

  Wanneer een publicatie of opmerking die spam, phishing of malware is, wordt gedetecteerd, ontvangt u een waarschuwingsbericht.
- waarschuwt uw vrienden voor verdachte koppelingen die op hun newsfeed zijn gepubliceerd.
- helpt u bij het opbouwen van een veilig netwerk van vrienden met de functie **FriendOMeter**.
- voer een controle uit van de status van de systeemveiligheid, geleverd door Bitdefender QuickScan.

Volg deze stappen om Safego te openen vanaf uw Bitdefender-product:

1. Open het Bitdefender-venster.
2. Ga naar het paneel **Safego**.
3. Klik op **Activeren**.U wordt naar uw account gebracht.

   Als u Safego al hebt geactiveerd, zult u de statistieken met betrekking tot zijn activiteiten kunnen openen door op de knop **Rapporten weergeven** te klikken.
4. Gebruik uw Facebook-aanmeldingsgegevens om een verbinding te maken met de Safego-toepassing.
5. Safego-toegang tot uw Facebook-account toestaan.

13. Problemen oplossen

Dit hoofdstuk beschrijft enkele problemen die zich kunnen voordoen terwijl u Bitdefender gebruikt en biedt u mogelijke oplossingen voor deze problemen.De meeste problemen kunnen worden opgelost door de juiste configuratie van de productinstellingen.

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Ondersteuning*" (p. 140).

13.1. Mijn systeem lijkt traag

Na het installeren van beveiligingssoftware kan er doorgaans een lichte vertraging van het systeem merkbaar zijn. Dit is normaal tot in zekere mate.

Als u een aanzienlijke vertraging opmerkt, kan dit probleem verschijnen door de volgende redenen:

- **Bitdefender is niet het enige beveiligingsprogramma dat op uw systeem is geïnstalleerd.**

  Hoewel Bitdefender de beveiligingsprogramma's verwijdert die tijdens de installatie zijn gevonden, is het aanbevolen elk ander antivirusprogramma dat u mogelijk gebruikt voordat u Bitdefender installeert, te verwijderen.Meer informatie vindt u onder "*Andere beveiligingsoplossingen verwijderen*" (p. 148).

- **Er is niet voldaan aan de minimale systeemvereisten voor het uitvoeren van Bitdefender.**

Als uw apparaat niet voldoet aan de minimale systeemvereisten, wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn.Meer informatie vindt u onder "*Minimale systeemvereisten*" (p. 2).

- **Uw harde schijven zijn te gefragmenteerd.**

  Bestandsfragmentatie vertraagt de bestandstoegang en verlaagt de systeemprestaties.

  Om de schijf te defragmenteren met uw Windows-besturingssysteem, volgt u het pad vanaf het Start-menu van Windows: **Start → Alle programma's → Bureau-accessoires → Systeemwerkset → Schijfdefragmentatie**.

13.2. Het scannen start niet

Dit probleemtype kan twee hoofdoorzaken hebben:

- **Een eerder installatie van Bitdefender die niet volledig werd verwijderd of een ongeldige Bitdefender-installatie**.

  Volg in dat geval de onderstaande stappen:

  1. Bitdefender volledig van het systeem verwijderen:
     a. Ga naar http://www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
     b. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.
     c. Start uw computer opnieuw op.
  2. Bitdefender opnieuw installeren op het systeem.

- **Bitdefender is niet de enige beveiligingsoplossing die op uw systeem is geïnstalleerd**.

  Volg in dat geval de onderstaande stappen:

  1. Verwijder de andere beveiligingsoplossing.Meer informatie vindt u onder "*Andere beveiligingsoplossingen verwijderen*" (p. 148).
  2. Bitdefender volledig van het systeem verwijderen:
     a. Ga naar http://www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
     b. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.
     c. Start uw computer opnieuw op.
  3. Bitdefender opnieuw installeren op het systeem.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

13.3. Ik kan de toepassing niet meer gebruiken

Dit probleem doet zich voor wanneer u probeert een programma te gebruiken dat normaal werkte vóór de installatie van Bitdefender.

Er kan zich een van de volgende situaties voordoen:

- U kunt van Bitdefender een bericht ontvangen met de melding dat het programma probeert een wijziging aan te brengen aan het systeem.
- U kunt een foutbericht ontvangen van het programma dat u probeert te gebruiken.

Dit soort situatie doet zich voor wanneer de module Actief virusbeheer sommige toepassingen verkeerdelijk identificeert als kwaadaardig.

Actief virusbeheer is een Bitdefender-module die de toepassingen op uw systeem voortdurend bewaakt en programma's met een potentieel boosaardig gedrag rapporteert.Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij rechtmatige toepassingen worden gerapporteerd door Actief virusbeheer.

Wanneer deze situatie zich voordoet, kunt u de respectieve toepassing uitsluiten van de bewaking door Actief virusbeheer.

Volg deze stappen om het programma toe te voegen aan de lijst met uitsluitingen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Uitsluitingen**.
4. Klik op de koppeling **Uitgesloten processen**.In het venster dat verschijnt, kunt u de uitsluitingen voor het proces Actief virusbeheer beheren.
5. Volg deze stappen om uitsluitingen toe te voegen:
   a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
   b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.
   c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief virusbeheer de toepassing blokkeert.
   d. Klik op **Toevoegen**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

13.4. Ik kan geen verbinding maken met internet

Het is mogelijk dat een programma of een webbrowser, na het installeren van Bitdefender, geen verbinding meer kan maken met internet of geen toegang meer krijgt tot de netwerkdiensten.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van de respectieve softwaretoepassing automatisch toe te staan.

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Firewallregels op **Toepassingsregels**.
5. Klik op de overeenkomende knop om een toepassingsregel toe te voegen.
6. Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt.
7. Selecteer alle beschikbare netwerktypes.
8. Ga naar **Machtiging** en selecteer **Toestaan**.

Sluit Bitdefender, open de softwaretoepassing en probeert opnieuw een verbinding te maken met internet.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

13.5. Ik kan geen toegang krijgen tot een apparaat op mijn netwerk.

Afhankelijk van het netwerk waarmee u verbonden bent, kan de Bitdefender-firewall de verbinding tussen uw systeem en een ander apparaat (zoals een andere computer of printer) blokkeren.Hierdoor zult u mogelijk niet langer bestanden kunnen delen of afdrukken.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van het respectieve apparaat automatisch toe te staan.Voor elke netwerkverbinding kunt u een speciale vertrouwde zone configureren.

Een vertrouwde zone is een apparaat dat u volledig vertrouwt.Al het verkeer tussen uw computer en het vertrouwde apparaat is toegestaan.Om bronnen met specifieke apparaten, zoals computers of printers te delen, voegt u ze toe als vertrouwde zones.

Volg deze stappen om een vertrouwde zone toe te voegen aan uw netwerkadapters:

1. Open het Bitdefender-venster.

2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Geavanceerd**.
4. Klik onder Firewallregels op **Adapterregels**.
5. Klik op de overeenkomende knop om een zone toe te voegen.Er wordt een nieuw venster weergegeven met de IP-adressen van de apparaten die met het netwerk zijn verbonden.
6. Selecteer het IP-adres van de computer of de printer die u wilt toevoegen of voer een adres of adresbereik in het opgegeven tekstvak in.
7. Ga naar **Machtiging** en selecteer **Toestaan**.

Als u nog steeds geen verbinding kunt maken met het apparaat, wordt het probleem mogelijk niet veroorzaakt door Bitdefender.

Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op de andere computer kan het delen van bestanden en printers met uw computer blokkeren.
  - Als de Windows Firewall wordt gebruikt, kan deze worden geconfigureerd om het delen van bestanden en printers als volgt toe te staan: open het venster met de instellingen van de Windows Firewall, klik op het tabblad **Uitzonderingen** en schakel het selectievakje **Bestands- en printerdeling** in.
  - Als er een ander firewall-programma wordt gebruikt, moet u de documenten of het Help-bestand van dit programma raadplegen.
- Algemene omstandigheden die het gebruik van of verbinden met de gedeelde printer kunnen verhinderen:
  - U moet zich mogelijk aanmelden bij een Windows-beheerdersaccount om toegang te krijgen tot de gedeelde printer.
  - Er zijn machtigingen ingesteld voor de gedeelde printer om de toegang alleen toe te staan tot specifieke computers en gebruikers.Als u uw printer deelt, moet u de machtigingen controleren die voor de printer zijn ingesteld om te zien of de gebruiker op de andere computer toegang heeft tot de printer.Als u probeert een verbinding te maken met een gedeelde printer, moet u bij de gebruiker op de andere computer controleren of u de machtiging hebt om een verbinding te maken met de printer.
  - De printer die op uw computer of op de andere computer is aangesloten, wordt niet gedeeld.
  - De gedeelde printer is niet toegevoegd aan de computer.

Opmerking

Om te leren hoe u het delen van printers kunt beheren (een printer delen, machtigingen voor een printer instellen of verwijderen, verbinden met een netwerkprinter of met een gedeelde printer), gaat u naar Windows Help en ondersteuning (klik in het menu Start op **Help en ondersteuning**).

- De toegang tot de netwerkprinter is mogelijk beperkt tot specifieke computers of gebruikers. Raadpleeg de netwerkbeheerder om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

13.6. Mijn internetverbinding is langzaam

Deze situatie kan zich voordoen nadat u Bitdefender hebt geïnstalleerd.Het probleem kan zijn veroorzaakt door fouten in de Bitdefender-firewallconfiguratie.

Volg de onderstaande stoppen om deze probleemsituatie op te lossen:

1. Open het Bitdefender-venster.
2. Ga naar het venster **Firewall** en klik op de schakelaar om deze optie uit te schakelen.
3. Controleer of uw internetverbinding verbetert wanneer de Bitdefender-firewall is uitgeschakeld.
   - Als u nog steeds een langzame internetverbinding kunt maken, wordt het probleem mogelijk niet veroorzaakt door Bitdefender. Neem contact op met uw internet-provider om te controleren of de verbinding werkt aan hun kant.

     Als u van uw internet-provider de bevestiging ontvangt dat de verbinding aan hun zijde werkt en het probleem zich blijft voordoen, neemt u contact op met Bitdefender zoals beschreven in sectie “*Hulp vragen*” (p. 141).
   - Volg deze stappen als de internetverbinding is verbeterd naar het uitschakelen van de Bitdefender-firewall:
     a. Open het Bitdefender-venster.
     b. Ga naar het venster **Firewall** en klik op de schakelaar om deze optie in te schakelen.
     c. Klik op de knop **Instellingen** in de werkbalk bovenaan.
     d. Klik in het menu aan de linkerzijde op **Firewall** en klik vervolgens op het tabblad **Instellingen**.
     e. Ga naar **Internetverbinding delen** en klik op de schakelaar om deze optie in te schakelen.

f. Ga naar **Poortscans blokkeren** en klik op de schakelaar om deze optie uit te schakelen.

g. Klik op de knop **Home** in de werkbalk bovenaan.

h. Ga naar het paneel **Firewall** en klik op **Netwerkdetails**.

i. Ga naar **Netwerktype** en selecteer **Thuis/Bureau**.

j. Ga naar **Stealth-modus** en stel deze in op **Extern**. Stel **Algemeen** in op **Ja**.

k. Sluit Bitdefender, start het systeem opnieuw op en controleer de snelheid van de internetverbinding.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

13.7. Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Volg deze stappen om uw systeem up-to-date te houden met de recentste Bitdefender-malwarehandtekeningen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Update** en klik vervolgens op het tabblad **Update**.
4. Selecteer onder **Regels voor behandelen updates** de optie **Herinneren voor het downloaden**.
5. Klik op de knop **Home** in de werkbalk bovenaan.
6. Open het venster **Update** en klik op **Nu bijwerken**.
7. Selecteer alleen **Updates handtekeningen** en klik vervolgens op **OK**.
8. Bitdefender zal alleen de updates van de malwarehandtekeningen downloaden en installeren.

13.8. Mijn computer is niet verbonden met internet. Bitdefender bijwerken

Als uw computer niet is verbonden met internet, moet u de updates handmatig downloaden naar een computer met internettoegang en ze vervolgens overdragen naar uw computer met een verwisselbaar apparaat, zoals een flashstation.

Volg deze stappen:

1. Open een webbrowser op een computer met internettoegang en ga naar:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. Klik in de kolom **Handmatige update** op de koppeling die overeenkomt met uw product en systeemarchitectuur.Raadpleeg *"Gebruik ik een 32- of 64-bits versie van Windows?"* (p. 149) als u niet weet of Windows op 32- of 64-bits wordt uitgevoerd.

3. Sla het bestand met de naam `weekly.exe` op het systeem op.

4. Draag het gedownloade bestand over naar een verwisselbaar apparaat, zoals een flashstation, en vervolgens naar uw computer.

5. Dubbelklik op het bestand en volg de stappen van de wizard.

13.9. De Bitdefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding **Bitdefender-services reageren niet**.U kunt deze fout aantreffen als volgt:

- Het Bitdefender-pictogram in het systeemvak wordt grijs weergegeven en u krijgt een melding dat de Bitdefender-services niet reageren.
- Het Bitdefender-venster geeft aan dat de Bitdefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- er wordt een belangrijke update geïnstalleerd.
- tijdelijke communicatiefouten tussen de Bitdefender-services.
- sommige Bitdefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als Bitdefender uitgevoerd.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert.De fout kan tijdelijk zijn.

2. Start de computer opnieuw op en wacht enkele ogenblikken tot Bitdefender is geladen. Open Bitdefender om te zien of de fout blijft bestaan.Het probleem wordt doorgaans opgelost door de computer opnieuw op te starten.

3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van Bitdefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens Bitdefender opnieuw te installeren.

   Meer informatie vindt u onder *"Andere beveiligingsoplossingen verwijderen"* (p. 148).

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel *"Hulp vragen"* (p. 141).

13.10. De antispamfilter werkt niet goed

Dit artikel helpt u bij het oplossen van de volgende problemen met betrekking tot de werking van de antispamfilter van Bitdefender:

- Een aantal rechtmatige e-mailberichten wordt gemarkeerd als [spam]..
- Talrijke spamberichten worden niet als dusdanig gemarkeerd door de antispam-filter.
- De antispam-filter detecteert geen enkel spambericht.

13.10.1. Rechtmatige berichten worden gemarkeerd als [spam]

Rechtmatige berichten worden als [spam] gemarkeerd omdat ze eruit zien als spam voor de antispamfilter van Bitdefender.U kunt dit probleem oplossen door de antispamfilter op de goede manier te configureren.

Bitdefender voegt de ontvangers van uw e-mailberichten automatisch toe aan uw vriendenlijst.De e-mailberichten die zijn ontvangen van de contactpersonen in de vriendenlijst, worden beschouwd als rechtmatig. Ze worden niet gecontroleerd door de antispamfilter en worden daarom ook nooit gemarkeerd als [spam].

De automatische configuratie van de vriendenlijst verhindert niet dat er detectiefouten optreden in deze situaties:

- U ontvangt veel gevraagde commerciële e-mail omdat u zich op verschillende websites hebt geabonneerd.In dit geval bestaat de oplossing eruit de e-mailadressen waarvan u dergelijke e-mailberichten ontvangt, toe te voegen aan de vriendenlijst.
- Een belangrijk deel van uw rechtmatige e-mail komt van mensen naar wie u nog nooit een e-mail hebt gestuurd, zoals klanten, potentiële zakenpartners en anderen.In dit geval zijn andere oplossingen vereist.

1. Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, worden de detectiefouten aangegeven.

   Opmerking

   Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk.Raadpleeg *"Ondersteunde e-mailclients en protocollen" (p. 67)* voor een complete lijst van ondersteunde e-mailclients.

2. Het antispambeschermingsniveau verlagen. Door het beschermingsniveau te verlagen, zal de antispamfilter meer spamaanduidingen nodig hebben om een e-mailbericht als spam te klasseren.Probeer deze oplossing alleen als er veel rechtmatige berichten (inclusief gevraagde commerciële berichten) onjuist worden gedetecteerd als spam.

Contactpersonen toevoegen aan de vriendenlijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van rechtmatige berichten gemakkelijk toevoegen aan de vriendenlijst.Volg deze stappen:

1. Selecteer in uw e-mailclient een e-mailbericht van de afzender die u wilt toevoegen aan de vriendenlijst.
2. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender.
3. U wordt gevraagd de adressen die aan de vriendenlijst zijn toegevoegd, te bevestigen.Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

Als u een andere e-mailclient gebruikt, kunt u contactpersonen toevoegen aan de vriendenlijst vanaf de Bitdefender-interface.Volg deze stappen:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antispam**.
3. Klik op **Beheren** en kies **Vrienden** in het menu.Een configuratievenster wordt weergegeven.
4. Voer het e-mailadres in waarop u e-mailberichten wilt ontvangen en klik daarna op **Toevoegen**.U kunt zoveel e-mailadressen toevoegen als u wilt.
5. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet zijn gemarkeerd als `[spam]`). Hierdoor helpt u de efficiëntie van de antispamfilter verbeteren.Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als `[spam]`.
4. Klik op de knop **Vriend toevoegen** in de antispam-werkbalk van Bitdefender om de afzender aan de vriendenlijst toe te voegen.U zult mogelijk op **OK** moeten klikken om te bevestigen.U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
5. Klik op de knop **Geen spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient).Het e-mailbericht wordt verplaatst naar de map Postvak IN.

Het antispambeschermingsniveau verlagen

Volg deze stappen om het antispambeschermingsniveau te verlagen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Ga in het menu aan de linkerzijde naar **Antispam**.
4. Verplaats de schuifregelaar omlaag op de schaal.

13.10.2. Veel spamberichten worden niet gedetecteerd

Als u veel spamberichten ontvangt die niet als [spam] zijn gemarkeerd, moet u de antispamfilter van Bitdefender configureren om de efficiëntie te verbeteren.

Probeer de volgende oplossingen:

1. Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, worden niet-gedetecteerde spamberichten aangegeven.

   Opmerking

   Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk.Raadpleeg *"Ondersteunde e-mailclients en protocollen"* (p. 67) voor een complete lijst van ondersteunde e-mailclients.

2. Spammers toevoegen aan de spammerslijst. De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als [spam].
3. Het antispambeschermingsniveau verhogen. Door het beschermingsniveau te verhogen, zal de antispamfilter minder spamaanduidingen nodig hebben om een e-mailbericht als spam te klasseren.

Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor helpt u de efficiëntie van de antispamfilter verbeteren.Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop  **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

Spammers toevoegen aan de spammerslijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van de spamberichten gemakkelijk toevoegen aan de spammerslijst.Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer de berichten die door Bitdefender zijn gemarkeerd als `[spam]`.
4. Klik op de knop **Spammer toevoegen** in de antispam-werkbalk van Bitdefender.
5. U wordt gevraagd de adressen die aan de spammerslijst zijn toegevoegd, te bevestigen.Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

Als u een andere e-mailclient gebruikt, kunt u spammers handmatig toevoegen aan de spammerslijst vanaf de Bitdefender-interface. Het is handig om dit alleen te doen wanneer u meerdere spamberichten hebt ontvangen van hetzelfde e-mailadres.Volg deze stappen:

1. Open het Bitdefender-venster.
2. Ga naar het deelvenster **Antispam**.
3. Klik op **Beheren** en kies **Spammers** in het menu.Een configuratievenster wordt weergegeven.
4. Voer het e-mailadres van de scanner in en klik daarna op **Toevoegen**.U kunt zoveel e-mailadressen toevoegen als u wilt.
5. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Het antispambeveiligingsniveau verhogen

Volg deze stappen om het antispambeschermingsniveau te verhogen:

1. Open het Bitdefender-venster.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerzijde op **Antispam**.
4. Verplaats de schuifregelaar omhoog op de schaal.

13.10.3. De antispamfilter detecteert geen enkel spambericht

Als er een spambericht als `[spam]` is gemarkeerd, kan er een probleem zijn met de antispamfilter van Bitdefender.Voordat u dit probleem probeert op te lossen, moet u controleren of het niet wordt veroorzaakt door een van de volgende omstandigheden:

- De antispambeveiliging wordt mogelijk uitgeschakeld.Om de antispam-beveiligingsstatus te controleren, opent u het Bitdefender-venster en schakelt u het selectievakje in het paneel **Antispam** in.

  Als Antispam is uitgeschakeld, is dit de oorzaak van uw probleem.Klik op de schakelaar om de antispambeveiliging in te schakelen.

- De antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol.Dit betekent het volgende:

  - E-mailberichten die zijn ontvangen via op het web gebaseerde e-mailservices (zoals Yahoo, Gmail, Hotmail of andere), worden op spam gefilterd door Bitdefender.
  - Als uw e-mailclient is geconfigureerd om e-mailberichten te ontvangen met een ander protocol dan POP3 (bijv. IMAP4), controleert de antispamfilter van Bitdefender deze berichten niet op spam.

  Opmerking

  POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver.Als u het protocol dat uw e-mailclient gebruikt om e-mailberichten te downloaden niet kent, kunt u dat vragen aan de persoon die uw e-mailclient heeft geconfigureerd.

- Bitdefender Internet Security 2012 scant geen POP3-verkeer van Lotus Notes.

Een mogelijke oplossing is het repareren of opnieuw installeren van het product. Het is echter mogelijk dat u contact wilt opnemen met Bitdefender voor ondersteuning, zoals beschreven in sectie “*Ondersteuning*” (p. 140).

13.11. Het verwijderen van Bitdefender is mislukt

Dit artikel helpt u bij het oplossen van fouten die zich kunnen voordoen bij het verwijderen van Bitdefender.Er zijn twee mogelijke situaties:

- Tijdens het verwijderen, verschijnt een foutvenster.Het scherm biedt een knop voor het uitvoeren van een hulpprogramma voor het verwijderen waarmee het systeem zal worden opgeruimd.
- De procedure voor het verwijderen blijft hangen, uw systeem loopt eventueel vast.Klik op **Annuleren** om het verwijderen af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van Bitdefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van Bitdefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden.

Volg deze stappen om Bitdefender volledig te verwijderen van uw systeem:

1. Ga naar http://www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
2. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.
3. Start uw computer opnieuw op.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 141).

13.12. Mijn systeem start niet op na het installeren van Bitdefender

Als u Bitdefender net hebt geïnstalleerd en het systeem niet langer opnieuw kunt opstarten in de normale modus, kunnen er verschillende redenen zijn voor dit probleem.

Dit wordt zee waarschijnlijk veroorzaakt door een eerdere installatie van Bitdefender die niet goed werd verwijderd of door een andere beveiligingsoplossing die nog steeds op het systeem aanwezig is.

U kunt elke situatie op de volgende manier aanpakken:

- **U had eerder een versie van Bitdefender en hebt deze niet correct verwijderd.**

  Volg deze stappen om dit op te lossen:

  1. Start uw systeem opnieuw op en ga naar de Veilige modus.Raadpleeg *"Opnieuw opstarten in Veilige modus"* (p. 149) voor meer informatie hierover.
  2. Bitdefender verwijderen van uw systeem:
     a. Ga naar http://www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
     b. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.
     c. Start uw computer opnieuw op.
  3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**

  Volg deze stappen om dit op te lossen:

  1. Start uw systeem opnieuw op en ga naar de Veilige modus.Raadpleeg *"Opnieuw opstarten in Veilige modus"* (p. 149) voor meer informatie hierover.
  2. Bitdefender verwijderen van uw systeem:

a. Ga naar http://www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.

b. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.

c. Start uw computer opnieuw op.

3. Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.
4. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.

Volg deze stappen om dit op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus.Raadpleeg “*Opnieuw opstarten in Veilige modus*” (p. 149) voor meer informatie hierover.
2. Gebruik de optie Systeemherstel van Windows om de computer te herstellen naar een eerdere datum voordat u het product Bitdefender installeert.Raadpleeg “*Systeemherstel gebruiken in Windows*” (p. 150) voor meer informatie hierover.
3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel “*Hulp vragen*” (p. 141).

14. Malware van uw systeem verwijderen

Malware kan uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het type malware-aanval.Omdat virussen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de malwareinfectie niet automatisch kan verwijderen van uw systeem.In dergelijke gevallen is uw tussenkomst vereist.

- "*Helpmodus Bitdefender* " (p. 131)
- "*Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?*" (p. 133)
- "*Een virus in een archief opruimen*" (p. 134)
- "*Een virus in een e-mailarchief opruimen*" (p. 135)
- "*Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?*" (p. 136)
- "*De geïnfecteerde bestanden van de Systeemvolume-informatie opruimen*" (p. 136)
- "*Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?*" (p. 138)
- "*Wat zijn de overgeslagen items in het scanlogboek?*" (p. 138)
- "*Wat zijn de overgecomprimeerde bestanden in het scanlogboek?*" (p. 139)
- "*Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?*" (p. 139)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Ondersteuning*" (p. 140).

14.1. Helpmodus Bitdefender

Helpmodus is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities buiten uw besturingssysteem kunt scannen en desinfecteren.

Zodra Bitdefender Internet Security 2012 is geïnstalleerd, kan de Helpmodus worden gebruikt, zelfs als u niet langer kunt opstarten in Windows.

Uw systeem starten in de Helpmodus

U kunt de Helpmodus op één of twee manieren openen:

Vanaf het Bitdefender-venster

Volg deze stappen om de Helpmodus direct vanaf Bitdefender te openen:

1. Ga naar het deelvenster **Antivirus**.
2. Klik op **Nu scannen** en selecteer **Helpmodus** in het vervolgkeuzemenu.

   Er wordt een bevestigingsvenster weergegeven. Klik op **Ja** om uw computer opnieuw op te starten.
3. Nadat de computer opnieuw is opgestart, verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren.Kies **Bitdefender Rescue Image** en druk op de **Enter**-toets om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
4. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt.Druk vervolgens opnieuw op **Enter**.

   Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

Start uw computer direct op in de Helpmodus

Als Windows niet langer start, kunt u met de onderstaande stappen uw computer direct opstarten in de Helpmodus van Bitdefender.

Opmerking

Deze methode is niet beschikbaar op computers met Windows XP.

1. Start / herstart uw computer en druk op uw toetsenbord op de **spatiebalk** voordat het Windows-logo verschijnt.
2. Er verschijnt een menu waarin u wordt gevraagd een besturingssysteem voor het opstarten te selecteren.Druk op **TAB** om naar het gebied Tools.Kies **Bitdefender Rescue Image** en druk op de **Enter**-toets om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
3. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt.Druk vervolgens opnieuw op **Enter**.

   Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in de Helpmodus

Volg deze stappen om uw systeem te scannen in de Helpmodus:

1. Open de Helpmodus zoals beschreven in “Uw systeem starten in de Helpmodus” (p. 131).
2. Het Bitdefender-logo verschijnt en het kopiëren van de antivirus-engines wordt gestart.
3. Een welkomstvenster wordt weergegeven.Klik op **Doorgaan**.
4. Er is een update van de antivirushandtekeningen gestart.

5. Nadat de update is voltooid, verschijnt het venster van de antivirusscanner van Bitdefender voor scannen op aanvraag.
6. Klik op **Nu scannen**, selecteer het scandoel in het venster dat verschijnt en klik op **Openen** om het scannen te starten.

   Het is aanbevolen de volledige Windows-partitie te scannen.

   Opmerking

   Wanneer u in de Helpmodus werkt, krijgt u te maken met partitienamen van het Linux-type.Schijfpartities zullen verschijnen als `sda1` die waarschijnlijk overeenstemmen met het station `(C:)` Partitie van het Windows-type, `sda2` overeenkomend met `(D:)` enz.

7. Wacht tot de scan is voltooid. Volg de instructies als er malware is gedetecteerd, om de bedreiging te verwijderen.
8. Om de Helpmodus af te sluiten, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad. Selecteer vervolgens **Afmelden** in het menu dat verschijnt en kies vervolgens of u de computer opnieuw wilt opstarten of uitschakelen.

14.2. Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?

U kunt op een van de volgende manieren controleren of er een virus op uw computer aanwezig is:

- U hebt uw computer gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een viruswaarschuwing laat u weten dat Bitdefender een of meerdere virussen op uw computer heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste malwarehandtekeningen beschikt en voer een Volledige systeemscan uit om het systeem te analyseren.

Selecteer de gewenste actie (desinfecteren, verwijderen, naar quarantaine verplaatsen) voor de geïnfecteerde items zodra de volledige scan is voltooid.

Waarschuwing

Als u vermoedt dat het bestand deel uitmaakt van het Windows-besturingssysteem of dat het geen geïnfecteerd bestand is, volgt u deze stappen niet en neemt u zo snel mogelijk contact op met de klantendienst van Bitdefender.

Als de geselecteerde actie niet kan worden ondernomen en het scanlogboek een infectie meldt die niet kan worden verwijderd, moet u de bestanden handmatig verwijderen.

De eerste methode kan worden gebruikt in de normale modus:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Open het Bitdefender-venster.
   b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
   c. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
   d. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
2. Verborgen objecten weergeven in Windows.Raadpleeg *"Verborgen objecten weergeven in Windows"* (p. 150) voor meer informatie hierover.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real time antivirusbeveiliging van Bitdefender in.

Volg deze stappen in het geval de infectie niet kan worden verwijderd met de eerste methode:

1. Start uw systeem opnieuw op en ga naar de Veilige modus.Raadpleeg *"Opnieuw opstarten in Veilige modus"* (p. 149) voor meer informatie hierover.
2. Verborgen objecten weergeven in Windows.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 141).

14.3. Een virus in een archief opruimen

Een archief is een bestand of een verzameling van bestanden dat is gecomprimeerd onder een speciale indeling om de benodigde schijfruimte voor het opslaan van de bestanden te beperken.

Sommige van deze formaten zijn open formaten. Hierdoor kan Bitdefender binnen deze formaten scannen en de geschikte acties ondernemen om ze te verwijderen.

Andere archiefformaten worden gedeeltelijk of volledig gesloten. Bitdefender kan alleen de aanwezigheid van virussen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een virus is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is het virus te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een virus dat in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat het virus bevat door een Volledige systeemscan uit te voeren.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Open het Bitdefender-venster.
   b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
   c. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.
   d. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
3. Ga naar de locatie van het archief en decomprimeer het met een archiveringstoepassing, zoals WinZip.
4. Identificeer het geïnfecteerde bestand en verwijder het.
5. Verwijder het originele archief zodat u zeker bent dat de infectie volledig is verwijderd.
6. Comprimeer de bestanden in een nieuw archief met een archiveringstoepassing zoals WinZip.
7. Schakel de real time antivirusbescherming van Bitdefender in en voer een Volledige systeemscan uit om zeker te zijn dat er geen andere infecties op het systeem aanwezig zijn.

Opmerking
Het is belangrijk dat u weet dat een virus dat is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat het virus moet worden gedecomprimeerd en uitgevoerd om uw systeem te kunnen infecteren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 141).

14.4. Een virus in een e-mailarchief opruimen

Bitdefender kan ook virussen identificeren in e-maildatabases en e-mailarchieven die op de schijf zijn opgeslagen.

Het is soms nodig het geïnfecteerde bestand te identificeren met de informatie die is opgegeven in het scanrapport en het handmatig te verwijderen.

Een virus dat in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Open het Bitdefender-venster.

b. Klik op de knop **Instellingen** in de werkbalk bovenaan.

c. Klik in het menu aan de linkerzijde op **Antivirus** en klik vervolgens op het tabblad **Shield**.

d. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.

3. Open het scanrapport en gebruik de identificatiegegevens (Onderwerp, Van, Aan) van de geïnfecteerde berichten om ze te zoeken in de e-mailclient.
4. De geïnfecteerde bestanden verwijderen.De meeste e-mailclients verplaatsen het verwijderde bericht ook naar een herstelmap van waar het kan worden hersteld.U moet controleren of dit bericht ook uit deze herstelmap is verwijderd.
5. Comprimeer de map die het geïnfecteerde bericht bevat.
   - In Outlook Express:Klik in het menu Bestand op Map en vervolgens op Alle mappen comprimeren.
   - In Microsoft Outlook:Klik in het menu Bestand op Gegevensbestandsbeheer.Selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen.Klik op Compact.
6. Schakel de real time antivirusbeveiliging van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie “*Hulp vragen*” (p. 141).

14.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?

U kunt vermoeden dat een bestand in uw systeem gevaarlijk is, ondanks het feit dat uw Bitdefender-product het niet heeft gedetecteerd.

Volg deze stappen om te controleren of uw systeem beschermd is:

1. Voer een **Volledige systeemscan** uit met Bitdefender.Raadpleeg “*Hoe kan ik mijn systeem scannen?*” (p. 32) voor meer informatie hierover.
2. Als het scanresultaat schoon lijkt, maar u nog steeds twijfels hebt en wilt zeker zijn over het bestand, moet u contact opnemen met onze experts zodat wij u kunnen helpen.

   Raadpleeg “*Hulp vragen*” (p. 141) voor meer informatie hierover.

14.6. De geïnfecteerde bestanden van de Systeemvolume-informatie opruimen

De map met informatie over systeemvolumes is een zone op uw harde schijf die door het besturingssysteem is gemaakt en door Windows wordt gebruikt voor het opslaan van belangrijke informatie met betrekking tot de systeemconfiguratie.

De Bitdefender-engines kunnen alle geïnfecteerde bestanden die door Systeemvolume-informatie zijn opgeslagen detecteren, maar omdat het om een beschermd gebied gaat is het mogelijk dat ze niet kunnen worden verwijderd.

De geïnfecteerde bestanden die worden gedetecteerd in de mappen Systeemherstel, verschijnen als volgt in het scanlogboek:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Om de geïnfecteerde bestanden in de gegevensopslag volledig en onmiddellijk te verwijderen, schakelt u de functie Systeemherstel uit en opnieuw in.

Wanneer Systeemherstel wordt uitgeschakeld, worden alle herstelpunten verwijderd.

Wanneer Systeemherstel opnieuw wordt ingeschakeld, worden nieuwe herstelpunten gemaakt zoals dat vereist wordt door de planning en de gebeurtenissen.

Volg de onderstaande stappen om Systeemherstel uit te schakelen:

- **Voor Windows XP:**
  1. Volg dit pad. **Start** → **Alle programma's** → **Bureau-accessoires** → **Systeemwerkset** → **Systeemherstel**.
  2. Klik op **Instellingen Systeemherstel** aan de linkerzijde van het venster.
  3. Schakel het selectievakje **Systeemherstel uitschakelen** in voor alle stations en klik op **Toepassen**.
  4. Wanneer u wordt gewaarschuwd dat alle bestaande herstelpunten worden verwijderd, klikt u op **Ja** om door te gaan.
  5. Om Systeemherstel in te schakelen, schakelt u het selectievakje **Systeemherstel uitschakelen** uit voor alle stations en klikt u op **Toepassen**.
- **Voor Windows Vista:**
  1. Volg dit pad. **Start** → **Configuratiescherm** → **Systeem en onderhoud** → **Systeem**
  2. Klik in het linkerpaneel op **Systeembeveiliging**.

     Als u wordt gevraagd naar een beheerderswachtwoord of bevestiging, voert u het wachtwoord in of antwoordt u bevestigend.
  3. Om Systeemherstel uit te schakelen, schakelt u de selectievakjes uit die overeenkomen met elk station en klikt u op **OK**.
  4. Om Systeemherstel in te schakelen, schakelt u de selectievakjes in die overeenkomen met elk station en klikt u op **OK**.
- **Voor Windows 7:**
  1. Klik op **Start**, klik met de rechtermuisknop op **Deze computer** en klik op **Eigenschappen**.

2. Klik op de koppeling **Systeembeveiliging** in het linkerdeelvenster.
3. Selecteer elke stationsletter in de opties van **Systeembeveiliging** en klik op **Configureren**.
4. Selecteer **Systeembeveiliging uitschakelen** en klik op **Toepassen**.
5. Klik op **Verwijderen**, klik op **Doorgaan** wanneer u dat wordt gevraagd en klik daarna op **OK**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 141).

14.7. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?

Dit is slechts een melding die aangeeft dat Bitdefender heeft gedetecteerd dat deze bestanden ofwel door een wachtwoord ofwel door een vorm van codering zijn beveiligd.

De meest gebruikelijke items die door een wachtwoord zijn beveiligd, zijn:

- Bestanden die bij een andere beveiligingsoplossing horen.
- Bestanden die bij het besturingssysteem horen.

Om de inhoud ook daadwerkelijk te scannen, moeten deze bestanden zijn opgehaald of op een andere manier zijn gedecodeerd.

Als deze inhoud zou worden uitgepakt, zou de real time scanner van Bitdefender ze automatisch scannen om uw computer beschermd te houden.Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

14.8. Wat zijn de overgeslagen items in het scanlogboek?

Alle bestanden die in het scanrapport als Overgeslagen worden weergegeven, zijn zuiver.

Voor betere prestaties scant Bitdefender geen bestanden die niet werden gewijzigd sinds de laatste scan.

14.9. Wat zijn de overgecomprimeerde bestanden in het scanlogboek?

Overgecomprimeerde items zijn elementen die niet kunnen worden opgehaald door de scanengine of elementen waarvoor de decoderingstijd te lang zou zijn waardoor het systeem onstabiel zou kunnen worden.

Overgecomprimeerd betekent dat het Bitdefender het scannen binnen dat archief heeft overgeslagen omdat het uitpakken ervan teveel systeembronnen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

14.10. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?

Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren.Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

Dit is doorgaans het geval met installatiebestanden die zijn gedownload vanaf onbetrouwbare websites.Als u zelf in een dergelijke situatie terechtkomt, downloadt u het installatiebestand vanaf de website van de fabrikant of een andere vertrouwde website.

15. Hulp vragen

15.1. Ondersteuning

Bitdefender streeft ernaar haar klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden.Als u problemen ondervindt met of vragen hebt over uw Bitdefender-product, kunt u meerdere online bronnen gebruiken om snel een oplossing of antwoord te vinden.Als u dat wenst, kunt u ook contact opnemen met de Bitdefender-klantenservice. Onze medewerkers van de ondersteuningsdienst zullen uw vragen snel beantwoorden en u alle hulp bieden die u nodig hebt.

15.1.1. Online bronnen

Er zijn meerdere online bronnen beschikbaar om u te helpen bij het oplossen van uw problemen en vragen met betrekking tot Bitdefender.

- Bitdefender-ondersteuningscentrum:http://www.bitdefender.nl/site/KnowledgeBase/consumer/
- Bitdefender-ondersteuningsforum:http://forum.bitdefender.com
- het Malware City-portaal voor computerbeveiliging:http://www.malwarecity.com

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

Bitdefender-ondersteuningscentrum

Het Bitdefender-ondersteuningscentrum is een online opslagplaats van informatie over Bitdefender-producten.Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over viruspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

Het Bitdefender-ondersteuningscentrum is toegankelijk voor het publiek en kan vrij worden doorzocht.De uitgebreide informatie die de database bevat is nog een middel om Bitdefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben.Alle geldige aanvragen voor informatie of foutrapporten die van Bitdefender-klanten komen, vinden uiteindelijk hun weg naar het Bitdefender-ondersteuningscentrum, als rapporten over het oplossen van problemen, “spiekbriefjes” om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender-ondersteuningscentrum is op elk ogenblik beschikbaar op http://www.bitdefender.nl/site/KnowledgeBase/consumer/.

Bitdefender-ondersteuningsforum

Het Bitdefender-ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen.

Als uw Bitdefender-product niet goed werkt, als het specifieke virussen niet van uw computer kan verwijderen of als u vragen hebt over de manier waarop het werkt, kunt u uw probleem of vraag op het forum plaatsen.

Bitdefender-ondersteuningstechnici controleren het forum en plaatsen nieuwe informatie om u te helpen. U kunt ook een antwoord of oplossing krijgen van een meer ervaren Bitdefender-gebruiker.

Voordat u uw probleem of vraag verzendt, moet u op het forum zoeken of er geen soortgelijk of verwant onderwerp is.

Het Bitdefender-ondersteuningsforum is beschikbaar op http://forum.bitdefender.com in 5 verschillende talen: Engels, Duits, Frans, Spaans en Roemeens.Klik op de koppeling **Home & Home Office Protection** om toegang te krijgen tot het gebied voor verbruiksproducten.

Malware City-portaal

Het Malware City-portaal is een rijke bron aan informatie over de computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw computer wordt blootgesteld wanneer u een verbinding met internet maakt (malware, phishing, spam, cybercriminelen).Via een nuttig woordenboek leer u de termen kennen met betrekking tot de computerbeveiliging.

Er worden regelmatig nieuwe artikels gepubliceerd om u op de hoogte te houden van de recentst opgespoorde bedreigingen, de huidige beveiligingstrends en andere informatie over de sector van computerbeveiliging.

De webpagina van Malware City is http://www.malwarecity.com.

15.1.2. Hulp vragen

De sectie **Problemen oplossen** biedt u de nodige informatie betreffende de vaakst voorkomende problemen tijdens het gebruik van dit product.

Als u de oplossing voor uw probleem niet in de geleverde middelen hebt gevonden, kunt u direct met ons contact opnemen:

- “Neem direct met ons contact op vanaf uw Bitdefender-product” (p. 142)
- “Neem contact op met ons via ons online Ondersteuningscentrum” (p. 142)

Belangrijk

Om contact op te nemen met de klantendienst van Bitdefender, moet u uw Bitdefender-product registreren.Meer informatie vindt u onder *“Productregistratie”* (p. 8).

Neem direct met ons contact op vanaf uw Bitdefender-product

Als u een actieve internetverbinding hebt, kunt u direct vanaf de productinterface contact opnemen met Bitdefender voor hulp.

Volg deze stappen:

1. Open het Bitdefender-venster.
2. Klik onderaan rechts in het venster op de koppeling **Help en ondersteuning**.
3. U hebt de volgende opties:
   - Lees de relevante artikels of documenten en probeer de voorgestelde oplossingen.
   - Start een zoekactie in onze database naar de informatie die u nodig hebt.
   - Gebruik de knop **Contact opnemen met ondersteuning** om het ondersteuningshulpprogramma te starten en contact op te nemen met de klantendienst.Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.
     a. Schakel het selectievakje voor de overeenkomst en klik op **Volgende**.
     b. Vul het verzendformulier in met de nodige gegevens:
        i. Voer uw e-mailadres in.
        ii. Voer uw volledige naam in.
        iii. Kies uw land in het overeenkomende menu.
        iv. Voer een beschrijving in van het probleem dat zich heeft voorgedaan.
     c. Wacht enkele minuten terwijl Bitdefender met het product verwante informatie verzamelt. Deze informatie zal onze technici helpen een oplossing voor uw probleem te vinden.
     d. Klik op **Voltooien** om de informatie te verzenden naar de klantendienst van Bitdefender. Wij nemen zo snel mogelijk contact op met u.

Neem contact op met ons via ons online Ondersteuningscentrum

Als u de benodigde informatie niet kunt openen met het Bitdefender-product, kunt u ons online ondersteuningscentrum raadplegen:

1. Ga naar http://www.bitdefender.nl/site/KnowledgeBase/consumer/.Het Ondersteuningscentrum van Bitdefender bevat talrijke artikelen met oplossingen voor problemen met betrekking tot Bitdefender.
2. Selecteer uw product in de kolom aan de linkerzijde en zoek het Bitdefender-ondersteuningscentrum voor artikels die een oplossing voor uw probleem kunnen bieden.
3. Lees de relevante artikels of documenten en probeer de voorgestelde oplossingen.

4. Als de oplossing uw probleem niet oplost, gebruikt u de koppeling in het artikel om contact op te nemen met de klantendienst van Bitdefender.
5. Neem via e-mail, chat of telefoon contact op met de medewerkers van de ondersteuningsdienst van Bitdefender.

15.1.3. Supportcentrum

De laboratoria van Editions Profil en Bitdefender garanderen een technische ondersteuning voor alle producten die door ons development team worden onderhouden. Het kan zijn dat we u in het kader van een technisch probleem zullen voorstellen de versie van uw product gratis op te waarderen.

Deze service biedt ondersteuning voor vragen of problemen die te maken hebben met standaardtoepassingen voor de eindgebruiker of voor bedrijven, zoals:

- Gepersonaliseerde configuraties van de BitDefender programma's.
- Gebruiksadviezen met betrekking tot individuele werkstations of eenvoudige netwerken.
- Technische problemen na de installatie van Bitdefender producten.
- Ondersteuning bij het bestrijden van malware-activiteiten op het systeem.
- Toegang tot onze site met veelgestelde vragen en tot onze site voor gepersonaliseerd onderhoud, die 24u/24 en 7d/7 bereikbaar is via: http://www.bitdefender.fr/site/KnowledgeBase/getSupport
- Toegang tot onze afdeling internationale ondersteuning, waar onze medewerkers 7d/7 en 365d/jr via online chat-sessies informatie verschaffen en oplossingen bieden. Om toegang te krijgen tot deze ondersteuning, dient u het volgende adres op te geven in uw internetbrowser: http://www.bitdefender.fr/site/KnowledgeBase/getSupport

  Let op: aangezien het hier gaat om een internationale service, wordt de ondersteuning voornamelijk in het Engels geboden.

Telefonische ondersteuning:

De laboratoria van Editions Profil en Bitdefender stellen alles in het werk om de toegang tot telefonische ondersteuning te kunnen garanderen, tijdens plaatselijke werkuren van maandag tot en met vrijdag, met uitzondering van feestdagen.

Telefonische toegang tot de laboratoria van Editions Profil en Bitdefender:

- **Belgium**: 070 35 83 04
- **Netherlands**: 020 788 61 50

Zorg voordat u ons belt dat u de volgende zaken binnen handbereik hebt:

- het licentienummer van uw BitDefender programma. Geef dit nummer door aan een van onze technici zodat hij kan nagaan op welk type ondersteuning u recht hebt.
- de actuele versie van uw besturingssysteem.
- informatie met betrekking tot de merken en modellen van alle op uw computer aangesloten randapparaten en van de software die in het geheugen is geladen of in gebruik is.

In het geval er een virus is ontdekt, kan de technicus u vragen om een lijst met technische informatie en bepaalde bestanden door te sturen, die mogelijkerwijs nodig zijn voor het stellen van een diagnose.

Indien een technicus u om foutmeldingen vraagt, geef dan de exacte inhoud door en het moment waarop de meldingen verschenen, de activiteiten die eraan voorafgingen en de stappen die u zelf reeds hebt ondernomen om het probleem op te lossen.

De technicus zal een strikte procedure opvolgen in een poging het probleem op te sporen.

De volgende elementen vallen niet binnen de service:

- Deze technische ondersteuning heeft geen betrekking op de toepassingen, installaties, de deïnstallatie, de overdracht, preventief onderhoud, de vorming, het beheer op afstand of andere softwareconfiguraties dan diegene die tijdens de interventie specifiek door onze technicus werden vermeld.
- De installatie, de instellingen, de optimalisering en de netwerkconfiguratie of de configuratie op afstand van toepassingen die niet binnen het kader van de geldende ondersteuning vallen.
- Back-ups van software/gegevens. De klant dient zelf een back-up te maken van alle gegevens, software en bestaande programma's die aanwezig zijn op de informatiesystemen waarop onze ondersteuning van toepassing is, alvorens enige dienstprestatie te laten uitvoeren door Editions Profil en Bitdefender.

Editions Profil of Bitdefender KUNNEN IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR HET VERLIES OF DE RECUPERATIE VAN GEGEVENS, PROGRAMMA'S, OF VOOR HET NIET KUNNEN BENUTTEN VAN SYSTEMEN OF VAN HET NETWERK.

Adviezen beperken zich enkel tot de gestelde vragen en zijn gebaseerd op de door de klant verschafte informatie. De problemen en mogelijke oplossingen kunnen afhangen van het type systeemomgeving en van een groot aantal andere variabelen waarvan Editions Profil of Bitdefender niet op de hoogte zijn.

Editions Profil of Bitdefender kunnen dan ook in geen geval aansprakelijk worden gesteld voor eventuele schade die voortvloeit uit het gebruik van de verschafte informatie.

Het kan zijn dat het systeem waarop de Bitdefender programma's moeten worden geïnstalleerd onstabiel is (eerdere virusinfecties, installatie van meerdere antivirus

- of beveiligingsprogramma's, etc.). In betreffende gevallen zal een technicus u mogelijkerwijze voorstellen eerst een onderhoudsbeurt op uw systeem te laten uitvoeren, alvorens het probleem kan worden opgelost.

De technische gegevens kunnen wijzigen op het moment dat er nieuwe gegevens beschikbaar zijn. Om die reden raden Editions Profil en Bitdefender u dan ook aan regelmatig onze site "Producten" te raadplegen, via http://www.bitdefender.nl voor upgrades, of onze site met veelgestelde vragen (FAQ) op http://www.bitdefender.nl/site/Main/contactus/.

Editions Profil en Bitdefender wijzen elke aansprakelijkheid af voor enige rechtstreekse, onrechtstreekse, bijzondere of accidentele schade, of voor gevolgschade die te wijten is aan het gebruik van de aan u verschafte informatie.

Indien een interventie ter plaatse noodzakelijk is, zal de technicus u meer gedetailleerde informatie verschaffen met betrekking tot de dichtstbijzijnde wederverkoper.

15.2. Contactinformatie

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 10 jaar heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel niet contact op te nemen met ons als u vragen hebt.

15.2.1. Webadressen

Sales department: bitdefender@editions-profil.eu
Ondersteuningscentrum:http://www.bitdefender.nl/site/KnowledgeBase/consumer/
Documentatie: documentation@bitdefender.com
Lokale verdelers:http://www.bitdefender.nl/partners/
Media relations: communication@editions-profil.eu
Virusverzendingen: virus_submission@bitdefender.com
Spamverzendingen: spam_submission@bitdefender.com
Misbruikmeldingen: abuse@bitdefender.com
Web: http://www.bitdefender.nl

15.2.2. Lokale verdelers

De lokale Bitdefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar http://www.bitdefender.nl/partners/.

2. De contactgegevens van de lokale Bitdefender-verdelers zouden automatisch moeten verschijnen. Als dat niet gebeurt, selecteert u het land waarin u zich bevindt om de informatie weer te geven.
3. Als u geen Bitdefender-verdeler in uw lang vindt, kunt u met ons contact opnemen via e-mail op bitdefender@editions-profil.eu.

15.2.3. Bitdefender-kantoren

De Bitdefender-kantoren zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak. Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

France - Nederland

Editions Profil
49, Rue de la Vanne
92120 Montrouge
Telefoon: (0)20.788.61.50
Verkoopsafdeling: bitdefender@editions-profil.eu
Technische ondersteuning: http://www.bitdefender.nl/site/Main/contactus/
Website product: http://www.bitdefender.nl

V.S.

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefoon (kantoor&verkoop): 1-954-776-6262
Verkoop: sales@bitdefender.com
Technische ondersteuning: http://www.bitdefender.com/help/
Web: http://www.bitdefender.nl

VK en Ierland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Telefoon: +44 (0) 8451-305096
Verkoop: sales@bitdefender.co.uk
Technische ondersteuning: http://www.bitdefender.co.uk/site/KnowledgeBase/supportCenter
Web: http://www.bitdefender.co.uk

Duitsland

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Kantoor: +49 2301 91 84 0
Verkoop: vertrieb@bitdefender.de
Technische ondersteuning: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Spanje

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefoon: +34 902 19 07 65
Verkoop: comercial@bitdefender.es
Technische ondersteuning: http://www.bitdefender.es/ayuda
Website: http://www.bitdefender.es

Roemenië

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefoon verkoop: +40 21 2063470
E-mail verkoop: sales@bitdefender.ro
Technische ondersteuning: http://www.bitdefender.ro/suport
Website: http://www.bitdefender.ro

16. Nuttige informatie

Dit hoofdstuk stelt enkele belangrijke procedures voor waarvan u zich moet bewust zijn voordat u begint met het oplossen van een technisch probleem.

Het oplossen van een technisch probleem in Bitdefender vereist wat kennis van Windows. De volgende stappen hebben daarom vooral betrekking op het Windows-besturingssysteem.

16.1. Andere beveiligingsoplossingen verwijderen

De hoofdreden voor het gebruik van een beveiligingsoplossing is het bieden van bescherming en veiligheid voor uw gegevens.Maar wat gebeurt er als er meerdere beveiligingsproducten aanwezig zijn op hetzelfde systeem?

Wanneer u meer dan één beveiligingsoplossing op dezelfde computer gebruikt, wordt het systeem onstabiel.Het installatieprogramma van Bitdefender Internet Security 2012 detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

Volg de onderstaande stappen als u de andere beveiligingsoplossingen niet hebt verwijderd tijdens de eerste installatie:

- Voor **Windows XP**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Software**.
  2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- Voor **Windows Vista** en **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.

3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Als u de andere beveiligingsoplossing niet van uw systeem kunt verwijderen, kunt u het hulpprogramma voor het verwijderen ophalen van de website van de verkoper of direct met hem contact opnemen voor richtlijnen betreffende het verwijderen.

16.2. Opnieuw opstarten in Veilige modus

De Veilige modus is een diagnostische gebruiksmodus die hoofdzakelijk wordt gebruikt om problemen op te lossen die de normale werking van Windows beïnvloeden.Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot virussen die verhinderen dat Windows normaal wordt gestart.In de Veilige modus werken slechts enkele toepassingen en laadt Windows alleen de basisbesturingsprogramma's en een minimum aan componenten van het besturingssysteem.Daarom zijn de meeste virussen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Windows in Veilige modus starten:

1. Start de computer opnieuw.
2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
5. Dit proces eindigt met een bevestigingsbericht.Klik op **OK** om te bevestigen.
6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.

16.3. Gebruik ik een 32- of 64-bits versie van Windows?

Volg de onderstaande stappen om uit te zoeken of u een 32-bits of 64-bits besturingssysteem hebt:

- Voor **Windows XP**:
  1. Klik op **Start**.
  2. Zoek **Deze computer** in het menu **Start**.
  3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
  4. Als u **x64 Edition** vindt onder **Systeem**, betekent dit dat u werkt met de 64-bits versie van Windows XP.

Als **x64 Edition** niet in de lijst staat, betekent dit dat u werkt met de 32-bits versie van Windows XP.

- Voor **Windows Vista** en **Windows 7**:
  1. Klik op **Start**.
  2. Zoek **Computer** in het menu **Start**.
  3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
  4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.

16.4. Systeemherstel gebruiken in Windows

Als u de computer niet in de normale modus kunt starten, kunt u opstarten in Veilige modus en Systeemherstel gebruiken om te herstellen naar een tijdstip waarop de computer kon starten zonder fouten.

Om Systeemherstel uit te voeren, moet u als beheerder zijn aangemeld bij Windows.

Volg deze stappen om Systeemherstel te gebruiken:

- In Windows XP:
  1. Bij Windows aanmelden in Veilige modus.
  2. Volg het pad vanaf het menu Start van Windows: **Start → Alle programma's → Systeemwerkset → Systeemherstel**.
  3. Klik op de pagina **Welkom bij Systeemherstel** om de optie **Mijn computer herstellen naar een eerder tijdstip** te selecteren en klik daarna op Volgende.
  4. Volg de stappen van de wizard en u zou in staat moeten zijn het systeem op te starten in normale modus.
- In Windows Vista en Windows 7:
  1. Bij Windows aanmelden in Veilige modus.
  2. Volg het pad vanaf het menu Start van Windows: **Alle programma's → Bureau-accessoires → Systeemwerkset → Systeemherstel**.
  3. Volg de stappen van de wizard en u zou in staat moeten zijn het systeem op te starten in normale modus.

16.5. Verborgen objecten weergeven in Windows

Deze stappen zijn nuttig in de gevallen waarin u te maken krijgt met een malware en u de geïnfecteerde bestanden die kunnen verborgen zijn, te vinden en te verwijderen.

Volg deze stappen om verborgen objecten weer te geven in Windows.

1. Klik op **Start**, ga naar **Configuratiescherm** en selecteer **Mapopties**.

2. Ga naar het tabblad **Weergave**.
3. Selecteer **Inhoud systeemmappen weergeven** (alleen voor Windows XP).
4. Selecteer **Verborgen bestanden en mappen weergeven**.
5. Schakel het selectievakje **Extensies voor bekende bestandstypen verbergen** uit.
6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
7. Klik op **Toepassen** en vervolgens op **OK**.

Woordenlijst

Achterdeur

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic.

ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het Internet sterk af.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archief

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Bestandsnaamextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsnaamextensies. Ze gebruiken doorgaans één tot drie letters (sommige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. De twee populairste browsers zijn Netscape Navigator en Microsoft Internet Explorer. Beide zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie weergeven met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Cookie

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het in sommige gevallen wel juist.

Downloaden

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Heuristisch

Een methode voor het identificeren van nieuwe virussen op basis van regels. Deze scanmethode steunt niet op specifieke virussignatures. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaand virus. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java-applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, geeft u de naam van het applet op en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt registreert.

Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macrovirus

Een type computervirus dat is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen.

Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mailclient

Een e-mailclient is een toepassing waarmee u e-mail kan verzenden en ontvangen.

Niet-heuristisch

Deze scanmethode steunt op specifieke virussignaturen. Het voordeel van de niet-heuristische scan is dat hij zich niet laat misleiden door iets dat kan lijken op een virus en dat hij geen vals alarm genereert.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Opstartitems

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of een toepassingsprogramma. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Opstartsector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Opstartsectorvirus

Een virus dat de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal het virus actief worden in het geheugen. Wanneer u daarna uw systeem opstart, zal het virus telkens in het geheugen actief zijn.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website voor het updaten van persoonlijke gegevens, zoals wachtwoorden en creditcard-, BSN- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Polymorf virus

Een virus dat zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien zij geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. Bitdefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is,

doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het Internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dit geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeembronnen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het Internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot virussen, maken ze geen kopie van zichzelf, maar ze kunnen wel even vernietigend zijn. Een van de meest verraderlijke types van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van virussen, maar dat in werkelijkheid virussen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatemodule waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Virus

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste virussen kunnen zichzelf ook dupliceren. Alle computervirussen zijn door de mens gemaakt. Een eenvoudig virus dat zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudig virus is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren; Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Virushandtekening

Het binaire patroon van een virus, dat wordt gebruikt door het antivirusprogramma om het virus te detecteren en uit te schakelen.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.